LifeSize® Gatekeeper™
User Guide

July 2008
Copyright Notice

2008 LifeSize Communications Inc, and its licensors. All rights reserved.

LifeSize Communications has made every effort to ensure that the information contained in this document is accurate and reliable, but assumes no responsibility for errors or omissions. Information in this document is subject to change without notice. Companies, names, and data used in examples herein are fictitious unless noted. This document contains copyrighted and proprietary information, which is protected by United States copyright laws and international treaty provisions. No part of the document may be reproduced or transmitted, in any form or by any means, electronic or mechanical, for any purpose, without the express written permission from LifeSize Communications.

Trademark Acknowledgments

LifeSize® is the trademark of LifeSize Communications Inc. All other trademarks are the property of their respective owners.Contacting Customer Support

If you have questions, concerns, or need assistance, contact your LifeSize Channel Partner.

Providing Customer Feedback

LifeSize Communications welcomes your comments regarding our products and services. If you have feedback about this or any LifeSize product, please send it to feedback@lifesize.com. Contact information for LifeSize Communications is as follows:

Method	Address
Internet	http://www.lifesize.com
E-mail	support@lifesize.com
Phone	(877) LIFESIZE or (877) 543-3749 (512) 347-9300
Fax	(512) 347-9301

CONTENTS

About This Manual

Conventions Used in this Manual xv

1 *LifeSize Gatekeeper Overview*

What's in this Chapter 1
What is the LifeSize Gatekeeper? 1
LifeSize Gatekeeper Environment 2
What the LifeSize Gatekeeper Provides 3
  Built-in Policies 3
  Enhanced Services 3

2 *Gatekeepers*

What's in this Chapter 19
H.323 Recommendation 19
H.323 Gatekeepers 20
Gatekeeper Procedures 21
Call Establishment 21
  Gatekeeper Discovery 21
  Gatekeeper Registration 22
  Location Request 22
  Admission Request 22
Routing H.225.0 Call Signaling Channels 22
Routing H.245 Control Channels 26
Call Termination 26
  Disengage Request 26

Unregistration Request 26
Support of Endpoints without RAS Capabilities 27

CONFIGURING THE LIFESIZE GATEKEEPER

3 *Working with the LifeSize Gatekeeper*

What's in this Chapter 31
Introducing the Web Interface 31
Requirements for the Web Interface 31
Accessing the Web Interface 32
Login Profiles 34
Configuration Interface 34
Sidebar 35
Toolbar 37
Global Configuration Tabs 38
Users Tab 38
Applications Tab 40
LifeSize Gatekeeper Configuration Tabs 41

4 *Status Tab*

About the Status Tab 43

5 *Settings Tab*

About the Settings Tab 45
Basics 46
What You Can Configure 47
Calls 50
About the H.245 Proxy 51
What You Can Configure 51
Configuring a Fixed Calling Party Number Alias 53

Capacity 54
What You Can Configure 55
Dial Plan 57
What You Can Configure 58
Supplementary Services 59
What You Can Configure 60
Logs 62
About the Log 62
Log File Format 63
What You Can Configure 64
Billing 65
What You Can Configure 66
Alert Indications 67
What You Can Configure 67
Adding and Modifying SNMP Traps Servers 71
LDAP 71
About LDAP 73
LifeSize Gatekeeper-LDAP Synchronization 74
What You Can Configure 74
External API 81
What You Can Configure 82
What You See 82
Connecting to an External Authorization Server 82
DNS 83
About DNS 83
Automatic E-mail Address Generation 83
What You Can Configure 84
Adding or Modifying DNS Server Details 86
Central Database 87
About the Central Database 87
Accessing the Central Database 88
What You Can Configure 88
Radius 89
Specifying Your Authentication Policy 89
Customizing Alias Formats 90
What You Can Configure 91

Adding or Modifying RADIUS Server Details 92
Security 93
About H.235 Security 93
What You Can Configure 94
Alternate Gatekeeper 95
About the Alternate Gatekeeper Feature 95
Windows IP Addressing 96
Alternate Gatekeeper IP Addressing 96
Sample Alternate Gatekeeper Configuration 97
Alternate Gatekeeper Procedure 99
Updating Static Information 101
Updating Dynamic Information 101
Routing Mode 101
IP Release 101
Configuring the Alternate Gatekeeper Function 102
What You Can Configure 102
Advanced 104
What You Can Configure 104

6 *Neighbors Tab*

About Neighbor Gatekeepers 111
About the Neighbors Tab 112
What You Can Configure 114
Adding or Modifying a Neighbor Gatekeeper 114

7 *Registration Restrictions Tab*

About the Registration Restrictions Tab 117
Alias Format 118
Adding or Modifying an Alias Format Rule 120
IP Subnet 121
Adding or Modifying an IP Subnet Rule 122

8 *Endpoints Tab*

About the Endpoints Tab 125
About Predefined Endpoints 125
Endpoints 127
- What You Can Configure 128
- Adding or Modifying a Predefined Endpoint 130
- Adding or Modifying an Endpoint Alias 134
- Viewing Properties of the Group to which an Endpoint Belongs 136
- Modifying Properties of an Online Endpoint 138

Groups 140
About Groups 140
- Group Permissions for Local Services 141
- Group Permissions for Global Services 141
- Adding or Modifying a Group 143
- Viewing Properties of Endpoints Belonging to a Group 146
- Adding or Modifying a Group Rule 149

9 *Services Tab*

About LifeSize Gatekeeper Services 155
- User-defined Services 156
- Built-in Services 156

About the Services Tab 159
- What You Can Configure 161
- Adding or Modifying LifeSize Gatekeeper User-Defined Services 162

Services Tab in Dial Plan version 2 164
Services 165
Global Services 165
- About Global Services 165
- What You Can Configure 167
- Adding or Modifying Global Services 167

10 *Bandwidth Policy Tab*

About the Bandwidth Policy Tab 169

About Subzones 169
What Are Subzones? 169
Why Use Subzones? 170
Subzones 170
What You Can Configure 171
Adding or Modifying Subzones 171
Adding or Modifying Subzone Rules 173
Bandwidth Policy 175
Sample Topology with Subzones 175
Subzone Rules 176
Applying Rules 177
Calculating Used Bandwidth 178
Dedicated Rules 178
Default Rules 180
Configuring Bandwidth Policy 180
What You Can Configure 181
Adding or Modifying Inter-subzone Rules 182
Viewing or Modifying the Default Inter-subzone Rule 185
Adding or Modifying Inter-zone Rules 186
Viewing or Modifying the Default Inter-zone Rule 189

11 *Call Control Tab*

About the Call Control Tab 191
What You Can Configure 192
Viewing Call Details 194
Enabling Third Party Call Control 197
Specifying Third Party Control Call Aliases 200
Viewing Third Party Call Control Details 204

12 *Forward & Fallback Tab*

About the Forward & Fallback Tab 207
About Call Forwarding 207
About Call Fallback 208
Forwarding 208

What You Can Configure 210
Adding or Modifying a Call Forwarding Rule 211
Fallback 213
What You Can Configure 214
Adding or Modifying a Call Fallback Rule 215

13 *Hierarchy Tab*

About the Hierarchical Gatekeeper Structure 219
About the Hierarchy Tab 220
Parent Gatekeeper 220
About Parent Filters 220
What You Can Configure 221
Adding or Modifying a Parent Filter 223
Neighbors 223
What You Can Configure 225
Adding or Modifying a Neighbor Gatekeeper 226
Children 228
What You Can Configure 229
Adding or Modifying a Child Gatekeeper 230
Adding or Modifying a Child Prefix 231

14 *Event Log Tab*

About the Event Log Tab 233

15 *Security Passwords Tab*

About the Security Passwords Tab 235
What You Can Configure 236
Adding or Modifying User Details 237

16 *Version Tab*

About the Version Tab 239
Viewing License Details 240

CONFIGURING THE LDAP SERVER

17 *Configuring the LDAP Server*

What's in this Chapter 243
LDAP Basics 244
Supported LDAP Servers 244
Supported LDAP Schemas 244
  Gatekeeper Schema 244
  H.350 Schema 245
Inside the Gatekeeper Schema 245
  LDAP Tree 245
Configuration Options for Supported LDAP Servers 247
  Automatic Configuration 247
  Manual Configuration 247
LDAP Configuration Tool 247
  Accessing the LDAP Configuration Tool 248
Automatic Configuration for Sun Java System, NDS or iPlanet Directory Server (Both Schemas) 249
  LDAP Schema and Relevant Folders Exist on the Server 250
  LDAP Schema and Relevant Folders Do Not Exist on the Server 251
Automatic Configuration for Microsoft ADS (Both Schemas) 252
Working with the Gatekeeper Schema 253
  Accessing the LDAP Tree 253
  Modifying the LDAP Tree 254
Manually Configuring the OpenLDAP Server (Gatekeeper Schema) 257
  Adding Entries to the LDAP Tree 257
  Modifying Entries in the LDAP Tree 259
  Deleting Entries from the LDAP Tree 260
  Viewing the Error Log 260
Manually Configuring the OpenLDAP Server (H.350 Schema) 260
  Adding Entries to the LDAP Tree 261
  Modifying Entries in the LDAP Tree 263

Deleting Entries from the LDAP Tree 263
Viewing the Error Log 263
Binding the LifeSize Gatekeeper to the LDAP Server 264

APPENDICES

APPENDIX A *Additional Installation Information*

What's in this Appendix 267
Installing the SNMP Service (Windows 2000/2003) 268
Configuring the SNMP Service (Windows 2000/2003) 268
Installing IIS 4 Subcomponents (Windows 2000) 270
Installing IIS 4 Subcomponents (Windows 2003) 272
Configuring IIS 4 Subcomponents (Windows 2000/2003) 274

APPENDIX B *LifeSize Gatekeeper CDR Structure*

What's in this Appendix 277
CDR Basics 277
Field Types 278
CDR Field Format 278
Fixed Length Fields 278
Variable Length Fields 279
Field Tags and Default Attributes 280
Field Numeric Options 286
Alias Tags 286
Party Number Tags 286
Call Model Tags 287
Endpoint Type Tags 287
Destination Zone 288
ARJ Reason Tags 288
Release Reason Tags 288
Generator Tags 290
Record Type Tags 290

H.450 Forward Type Tags 290
H.450 Call Record Type Tags 291
Notes 291
CDR Samples 292
CDR for a Standard Call 292
CDR for a Forwarded Call 293
CDR for a Call to a Service 295

APPENDIX C *LifeSize Gatekeeper Group Hunting*

What's in this Appendix 299
Overview 299
Before You Begin 299
Configuring Group Hunting 300

APPENDIX D *LifeSize Gatekeeper Dial Plan version 2*

What's in this Appendix 301
Overview 301
Understanding Your Network 302
What Kind of Network Do You Have? 302
Gatekeeper Topology 303
Numbering 305
Prefixes 306
Services 307
Zone Prefixes 308
Exit Zone Prefixes 308
Stripping 308
Parent Filters 311
Implementation Example 313

APPENDIX E *Predefined Endpoint Authentication by Alias*

What's in this Appendix 315
Before You Begin 315

Alias Authentication in DHCP Mode 316
Alias Authentication in non-DHCP Mode 317
Alias Authentication in DHCP Mode using LDAP 318
Alias Authentication in non-DHCP Mode using LDAP 319
Examples 320

APPENDIX F *Troubleshooting the LifeSize Gatekeeper*

Resolving Endpoint Registration Failure 322
Resolving Endpoint Unregistration/Reregistration 323
Resolving H.323 Entity Registration Failure 323
Resolving Endpoint Connectivity Problems 324
Resolving Failure to Connect with the LDAP Server 324
Resolving Call Failure to Endpoints 325
Resolving Failure of Calls to the LifeSize Multipoint or LifeSize Gateway 326
Resolving Call Disconnection 327
Resolving Make Call Option Failure 327
Resolving Forwarding Rule Failure 327
Resolving Group Bandwidth Limitation Failure 328
Resolving Alternate Gatekeeper Option Failure 328

Index 331

ABOUT THIS MANUAL

CONVENTIONS USED IN THIS MANUAL

This manual uses the following conventions:

Convention	Description
Blue Headings in Upper Case	Level 1 headings introducing major sections.
☞	Pointing hand icon introduces a procedure.
orange link	Live links appear in orange.

1

LIFESIZE GATEKEEPER OVERVIEW

WHAT'S IN THIS CHAPTER

This chapter describes the LifeSize Gatekeeper environment and its unique features, including the following:

- What is the LifeSize Gatekeeper?
- LifeSize Gatekeeper Environment
- What the LifeSize Gatekeeper Provides

WHAT IS THE LIFESIZE GATEKEEPER?

The LifeSize Gatekeeper is a simple-to-use, ITU-T H.323 version 5-compliant gatekeeper application that is essential for the management of IP telephony and multimedia communication networks. The LifeSize Gatekeeper runs on the Windows 2000 Professional, Windows 2000 Server and Windows 2003 Server platforms.

Designed with the network manager in mind, the LifeSize Gatekeeper provides complete functionality for defining and controlling voice and video traffic management over IP networks. Network managers can configure, monitor and manage the activities of registered network users. Managers can set policies and control network resources such as bandwidth usage to ensure optimal implementation.

This flexible and scalable gatekeeper application can accommodate the growing needs of a continuously expanding networking environment. The LifeSize Gatekeeper supports up to 50 calls and 250 registrations according to the license purchased. It is designed to provide the necessary performance for high call volume carrier-class networks.

LIFESIZE GATEKEEPER ENVIRONMENT

The LifeSize Gatekeeper system consists of three main entities:

- The LifeSize Gatekeeper application that works together with the underlying LifeSize software—the Gatekeeper Core, H.341 MIB Stack and the H.323 Protocol Stack.
- A web server together with a web browser.
- SNMP services.

Figure 1-1 *The LifeSize Gatekeeper Environment*

Each numbered component in the LifeSize Gatekeeper environment performs a specific activity. The flow of information between components is as follows:

1. A user interacts with the LifeSize Gatekeeper via a web browser.
2. The browser sends and receives data (via HTTP) to a web server, which is an SNMP agent.
3. The web server sends and receives data to and from the LifeSize Gatekeeper using SNMP services.
4. The LifeSize Gatekeeper processes the data.
5. The Gatekeeper Core manages the gatekeeper activities.
6. The H.341 MIB manages the MIB data.
7. The Stack manages the sending and receiving of H.323 messages.

What the LifeSize Gatekeeper Provides

The LifeSize Gatekeeper is a fully compliant H.323 version 5 gatekeeper and provides all the functionality described in the H.323 Recommendation.

Built-in Policies

In addition to the standard gatekeeper capabilities, a set of built-in policies[1] enables the LifeSize Gatekeeper to provide the following enhanced functionality:

- Admission Control
- Address Translation
- Direct and Routed Modes
- Polling endpoint status mechanism using IRQ
- Call Authorization
- Bandwidth Management

Enhanced Services

The LifeSize Gatekeeper has many features providing enhanced facilities and services. LifeSize Gatekeeper features include:

- A web interface for configuring and administering the LifeSize Gatekeeper.
- CDR for customized billing solutions.
- H.341 MIB support.
- H.450 Forwarding and Transfer Supplementary Services.
- Cisco Proxy support.
- RAI/RAC support for load balancing.
- Line Hunting, Group Hunting and Conference Hunting.
- Resolution of unrecognized aliases (via inter-zone LRQ communication and LDAP).
- LDAP support.
- Domain Name Server support.
- Online logging.
- Dial Plan for hierarchical gatekeeper deployments.
- Wildcard digit manipulation.
- Alternate Gatekeeper for LifeSize Gatekeeper redundancy.

1. See Gatekeeper Procedures in the Gatekeepers chapter.

- H.235 security.
- Automatic LifeSize Multipoint service registration.
- Advanced Call Fallback mechanisms including IP-to-ISDN fallback.
- Inter-zone bandwidth management.
- TTL Resiliency.
- Fixed Calling Party Number.
- Force Direct Mode for service calls.
- H.245 Tunneling.
- Third Party Call Control.
- Manual definition of the number of alias matches necessary for successful authentication and registration of predefined endpoints.
- Endpoint registration restriction via E.164 alias and IP subnet.
- H.450 Forwarding when an activating endpoint is not registered to the LifeSize Gatekeeper.
- RADIUS server support for authentication and billing.
- Support for communication via XML messages with external authorization servers and third party call control client applications.
- H.350 standard support.
- User groups for easy management.
- Support for multiple subzones within the LifeSize Gatekeeper zone, allowing bandwidth control between each subzone.
- Enhanced SNMP trap support allows SNMP traps to be sent to multiple server destinations.
- IP address dialing control.
- Caller ID presentation control.
- Flat Index add-on for LRQ searches between Neighbor Gatekeepers.

Web Interface

The LifeSize Gatekeeper Administrator provides a single point of entry for LifeSize Gatekeeper configuration. For more information, see the Working with the LifeSize Gatekeeper chapter.

CDR

The LifeSize Gatekeeper builds Call Detail Records (CDRs) in a simple text format that can be used as input to third party billing programs or other software. For details of the CDR structure, see the LifeSize Gatekeeper CDR Structure appendix.

H.341 MIB Support

A Management Information Base (MIB) is a formal description of a set of network objects that can be managed using SNMP. The format of the MIB is defined as part of SNMP. The H.323 MIB extension is described in the ITU-T Draft Recommendation H.341 (May 1999), Multimedia Management Information Base for H.323 version 2. The LifeSize Gatekeeper supports the H.341 standard node for Registration, Admission and Signaling (RAS). This node contains three tables, one for each of the RAS parameters.

H.450 Forwarding and Transfer

A Supplementary Service is the collective set of operations that are carried out to perform a Supplementary Service process as defined in the H.450.x Recommendations. The LifeSize Gatekeeper defines two types of services: Call Forwarding and Call Transfer.

A Supplementary Service is created when:

- A Q.931 message containing an H.450 APDU[1] arrives across the network.
- The suitable condition for performing a service is implemented.

The protocols that support Supplementary Services are specified in a number of ITU-T Recommendations starting from H.450.1 and up, as each new Supplementary Service is defined. The ITU-T Recommendations relevant to the Supplementary Services supported by the LifeSize Gatekeeper are defined below.

Note Full details about the H.450.x Recommendations are available in the appropriate ITU-T Recommendations.

1. APDUs convey a sequence of H.450 messages from the caller to the receiver and back. The APDU sequence is an octet string and it is conveyed in the User-user information element of Q.931. The APDUs of H.450 are transparent to Q.931; the Q.931 does not know the structure of H.450 APDUs, nor does it analyze the string.

H.450.1

Recommendation H.450.1 defines the signaling protocol between H.323 entities for the control of Supplementary Services. The generic functional protocol defined in Recommendation H.450 provides the means of exchanging signaling information for the control of Supplementary Services over an IP network. This recommendation does not control any Supplementary Services but rather provides generic services to specific Supplementary Services Control entities. The generic functional protocol operates in conjunction with the Call Signaling Protocol defined in H.225.0. The protocol provides mechanisms for the support of Supplementary Services that may relate to existing H.323 calls, or are entirely independent of any existing H.323 calls.

H.450.2

Recommendation H.450.2 describes the procedures and the signaling protocol for the Call Transfer Supplementary Service in H.323 networks. The Call Transfer Supplementary Service enables user A to transform an existing call (from user A to user B) into a new call between user B and a user C, selected by user A.

H.450.3

Recommendation H.450.3 specifies the Call Diversion Supplementary Services which comprise the Call Forwarding Unconditional (CFU), Call Forwarding Busy (CFB), Call Forwarding No Reply (CFNR) and Call Deflection services, all of which are applicable to various basic services supported by H.323 endpoints. The Call Diversion Supplementary Services apply during call establishment, providing a diversion of an incoming call to another destination endpoint before the call is established. They apply to point-to-point calls.

Cisco Proxy Support

The Cisco Proxy is a device that acts as a gateway and relays H.323 data between H.323 zones. A Proxy registers with a gatekeeper, thereby becoming part of the zone of that gatekeeper. The Proxy isolates endpoints of different zones by concealing their addresses. The only addresses that are revealed are those of the LifeSize Gatekeeper and Proxy. During Call Setup, the gatekeepers in each zone obtain address information from each other. The Proxies use the address information from the LifeSize Gatekeeper applications to route the call between zones. In this way, endpoints in different zones cannot see each other directly, they only see each other's Proxy address.

For information about configuring the Cisco Proxy, see Advanced on page 104, the Neighbors Tab chapter and the Hierarchy Tab chapter.

RAI/RAC, Line Hunting, Group Hunting and Conference Hunting

RAI/RAC

The Resource Available Indication/Resource Available Confirmation (RAI/RAC) function automatically manages load balancing on the network.

RAI/RAC messages are exchanged between the LifeSize Gatekeeper and a gateway to determine whether the gateway is available to receive calls. A gateway sends a RAI message to notify the LifeSize Gatekeeper of the current availability of the gateway for each H-series protocol. The LifeSize Gatekeeper responds with a RAC message to acknowledge receipt of a RAI message.

If the gateway is unavailable, the LifeSize Gatekeeper routes the call to an alternative available gateway.

Line Hunting

A gateway supports a list of prefixes (services). When a gateway is unavailable to receive a call, this means that it cannot accept calls with the particular prefix in question. The LifeSize Gatekeeper activates the Line Hunting function and searches for a gateway which is free to accept calls with this prefix.

When the LifeSize Gatekeeper receives an indication from a gateway in the RAI message that the gateway (the *specified* gateway) is almost at maximum capacity, the LifeSize Gatekeeper marks the services of that gateway as “almost out of resources”. During the first round of Line Hunting, the LifeSize Gatekeeper ignores this specified gateway when searching for the indicated gateway service.

If the LifeSize Gatekeeper cannot find a gateway which can accept a call with a specific prefix in this first round of searching, the LifeSize Gatekeeper can return to the first gateway it checked (the *specified* gateway) and begin a second round of searching for an available gateway. In this second round, the LifeSize Gatekeeper ignores the “almost out of resources” flag and tries *all* gateways in searching for a gateway to take the call. If the LifeSize Gatekeeper does not find a service provider (an available gateway) in the second round of searching, the call is rejected. If no other gateway with the same service is available in the zone, the LifeSize Gatekeeper routes the call to the specified gateway, as shown in Figure 1-2 on page 8.

Note If the LifeSize Gatekeeper cannot complete a call, the call is rejected unless relevant Call Forwarding or Call Fallback rules exist. For information on configuring Call Forwarding and Call Fallback rules, see the Forward & Fallback Tab chapter.

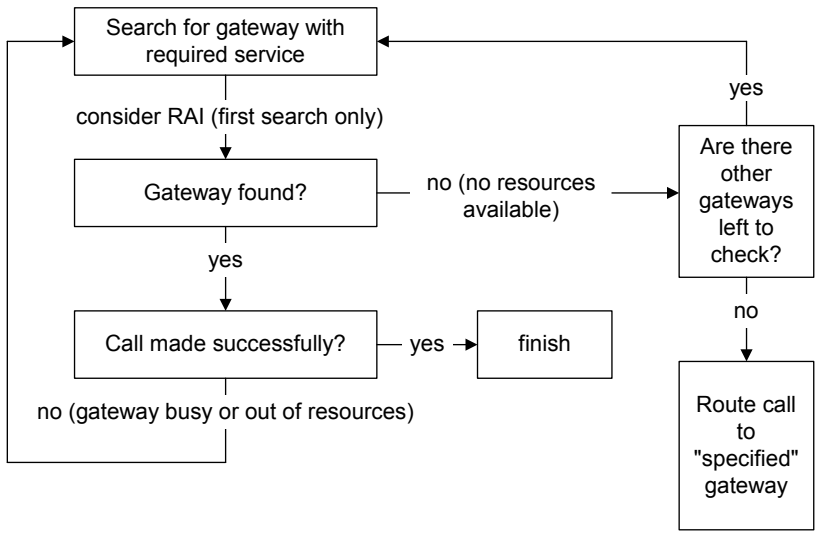

Figure 1-2 *Line Hunting Flow Chart*

GROUP HUNTING

Group Hunting enables the LifeSize Gatekeeper to perform load balancing for a group of endpoints. To achieve this, you define an alias for several H.323 endpoints thereby grouping them together. The LifeSize Gatekeeper hunts for the first endpoint in the group. If this endpoint is available, the endpoint accepts the call. If this endpoint is not available, the LifeSize Gatekeeper directs the call to the next endpoint in the group and so on in a “round robin” fashion. A range of aliases defines several different groups.

A group alias can be the existing online alias of one of the members of the group, or you can configure a new predefined alias for all the endpoints in the group. For more information about configuring Group Hunting, see the LifeSize Gatekeeper Group Hunting appendix.

Conference Hunting

The LifeSize Gatekeeper supports Conference Hunting. The purpose of Conference Hunting is to maintain conferences and ignore Line Hunting where necessary.

LifeSize Multipoint calls consist of a service prefix followed by a password (or conference ID). In order to create a conference, all calls with the same password (or conference ID) have to be directed to the same LifeSize Multipoint. If a password (or conference ID) is new, Conference Hunting takes place in *all* LifeSize Multipoints in the zone.

When the LifeSize Gatekeeper receives a call with the same prefix as an existing call, the LifeSize Gatekeeper directs the new call to the same service provider (LifeSize Multipoint) as the existing call. If the service provider refuses the call, the LifeSize Gatekeeper does not attempt Line Hunting. This scenario also overrides RAI indications.

For example, prefix 78 is configured to be of Conference Hunting type. Assume a call is made to this prefix with the number 78111. If another call with the same number (78111) is made, the gatekeeper will direct the second call to the same LifeSize Multipoint. If the LifeSize Multipoint refuses to accept the call, Line Hunting does not take place.

Resolution of Aliases

The LifeSize Gatekeeper resolves aliases that are not in the LifeSize Gatekeeper registration database by sending an LRQ first to the LDAP server, then to a DNS server, then to the Neighbor Gatekeepers that appear in the **Neighbors** tab, and finally by using multicast. To instruct the LifeSize Gatekeeper to send an LRQ to each of these destinations, you must configure each destination separately. You can also configure the LifeSize Gatekeeper to send an LRQ simultaneously to all the destinations listed above.

When the **Dial Plan** field in the **Basics** section of the **Settings** tab is set to **Version 2**, the **Hierarchy** tab replaces the **Neighbors** tab. In such cases the LifeSize Gatekeeper sends an LRQ to the Neighbor Gatekeepers that appear in the **Neighbors** section of the **Hierarchy** tab instead of to the Neighbor Gatekeepers that appear in the **Neighbors** tab.

For more information about including specific databases in the LRQ policy of the LifeSize Gatekeeper, see the following:

- LDAP server—See LDAP on page 71.
- DNS server—See DNS on page 83.
- Neighbor Gatekeepers—See the Neighbors Tab chapter and the Hierarchy Tab chapter.

- Multicast—See Basics on page 46.
- All destinations simultaneously—See Advanced on page 104.

LDAP Support

The Lightweight Directory Access Protocol (LDAP) is a protocol for accessing online directory services. LDAP is both an information model and a protocol for querying and manipulating the model.

A special LifeSize LDAP client plug-in that is part of the LifeSize Gatekeeper is used for retrieving information from a dedicated LDAP server, for permitting or denying service, or for routing calls.

The LDAP Plug-in defines some entry structures, sets user and gatekeeper information in these structures, and stores them in an LDAP server. The information stored in the LDAP server is then used by the LifeSize Gatekeeper Plug-in for address resolution. For more information, see LDAP on page 71 and the Configuring the LDAP Server chapter.

Domain Name Server Support

The LifeSize Gatekeeper can contact a pre-configured DNS server to resolve unrecognized aliases and receive a list of gatekeepers relevant to the queried domain. For more information about DNS server support, see DNS on page 83.

Online Logging

The LifeSize Gatekeeper provides an online window containing all LifeSize Gatekeeper logging information. For more information about online logging, see Logs on page 62.

Dial Plan

Version 2 of the LifeSize Gatekeeper Dial Plan enables you to configure gatekeepers in a flat and/or hierarchical topology to enable efficient location of called endpoints. For more information about the version 2 Dial Plan, see Dial Plan on page 57 and the LifeSize Gatekeeper Dial Plan version 2 appendix.

Wildcard Digit Manipulation

Wildcard Digit Manipulation enables the LifeSize Gatekeeper to manipulate an incoming call destination number before searching for the destination endpoint. For more information about digit manipulation, see Advanced on page 104.

High Availability via Alternate Gatekeeper

The Alternate Gatekeeper feature enables you to configure a backup LifeSize Gatekeeper (the Alternate Gatekeeper) for each LifeSize Gatekeeper gatekeeper. For more information about the Alternate Gatekeeper feature, see Alternate Gatekeeper on page 95.

H.235 Security

The LifeSize Gatekeeper supports H.235 security. For more information about security, see Security on page 93.

Automatic LifeSize Multipoint Service Registration

To simplify interworking between LifeSize elements, an LifeSize Multipoint can automatically register services to the LifeSize Gatekeeper.

Automatic registration of LifeSize Multipoint services occurs when the **MCU** option is selected in the **RgstrMode** advanced command of the LifeSize Multipoint.

The new LifeSize Multipoint services are automatically registered to the LifeSize Gatekeeper and appear in the **Services** tab. When the LifeSize Multipoint unregisters from the LifeSize Gatekeeper, all the LifeSize Multipoint services are deleted from the **Services** tab unless the administrator modifies the configuration of one of the services.

Automatic E-mail Address Generation

The LifeSize Gatekeeper can automatically generate an e-mail alias according to the domain configured in the **Local Domain** field of the **DNS** section of the **Settings** tab. This enables the LifeSize Gatekeeper Domain Name Server to resolve e-mail aliases even when an endpoint does not support e-mail alias definition.

The LifeSize Gatekeeper generates an e-mail alias as follows:

RRQ MESSAGES

- When the H.323 Name alias contains the "@" symbol:

  The LifeSize Gatekeeper generates an e-mail address by copying the H.323 alias. This e-mail address is added to the current list of e-mail addresses. The new e-mail address does not override an existing identical address in the list.

- When the H.323 Name alias does not contain the "@" symbol:

  The LifeSize Gatekeeper generates an e-mail using the format

  <h323 ID>@<gatekeeper domain>

  where

  - *h323 ID* represents the H.323 Name alias.
  - *gatekeeper domain* represents the value entered in the **Local Domain** field of the **DNS** section of the **Settings** tab.

ARQ AND LRQ MESSAGES

- When the H.323 Name alias contains the "@" symbol:

  The LifeSize Gatekeeper generates an e-mail address by copying the H.323 alias. This e-mail address is added to the current list of e-mail addresses. The new e-mail address does not override an existing identical address in the list.
- When the H.323 Name alias does not contain the "@" symbol:

  The LifeSize Gatekeeper takes no action.

For information about configuring the automatic generation of e-mail addresses, see DNS on page 83.

TIME-TO-LIVE (TTL) AND TTL RESILIENCY

TTL

The Time-to-Live (TTL) feature provides enabled registrations management and ensures that information displayed in the LifeSize Gatekeeper Administrator user interface accurately reflects the LifeSize Gatekeeper database.

TTL forces a registered endpoint to re-register with the LifeSize Gatekeeper when the endpoint TTL setting expires. When the TTL feature is unchecked, the LifeSize Gatekeeper ignores the endpoint TTL setting and regards that endpoint as being online, even after the endpoint TTL setting expires. For information about the TTL feature, see Advanced on page 104.

TTL RESILIENCY

TTL Resiliency ensures that TTL messages safely reach the LifeSize Gatekeeper in cases where there is noise on the network.

TTL Resiliency enables administrators to increase the length of time that the LifeSize Gatekeeper waits for a TTL before an endpoint is unregistered. For information about configuring TTL Resiliency, see Advanced on page 104.

Fixed Calling Party Number

The Fixed Calling Party Number (CPN) feature enables administrators to assign a fixed Calling Party Number to an alias which is predefined in the LifeSize Gatekeeper in static IP mode. The CPN alias is based on the E.164 address of a specific endpoint. The *CallingPartyNumber* parameter can be used for billing purposes and is added to the CDR when the CDR is generated.

Administrators define predefined endpoints in a static IP mode with a permanent alias. The permanent alias is sent to the gateway and to the LifeSize Gatekeeper CDR. Users may change their own alias manually on the terminal, but the reported alias is defined according to the IP address and the predefined CPN.

Note The mapping between the source and the CPN alias is activated by defined sources only.

For information about configuring the Fixed Calling Party Number feature, see Calls on page 50, Advanced on page 104 and Adding or Modifying a Predefined Endpoint on page 130.

Force Direct Mode For Service Calls

When processing calls to a service (such as a gateway or LifeSize Multipoint), the LifeSize Gatekeeper automatically operates in Call Setup (Q.931) Mode. Checking the **Force Direct Mode for service calls** option forces the LifeSize Gatekeeper to operate in Direct Mode when processing calls to a service.

Warning Do not use the **Force Direct Mode for service calls** option when using the LifeSize Gatekeeper with a LifeSize Multipoint or a LifeSize Gateway. The Call Fallback feature and the Line Hunting, Conference Hunting and Group Hunting features do not work when you select the **Force Direct Mode for service calls** option.

To enable the **Force Direct Mode for service calls** option, see Advanced on page 104. For more information about routing modes, see Calls on page 50.

H.245 Tunneling

Support for the H.245 tunneling feature decreases the time between the point at which an endpoint initiates a call and the point at which the call participants are ready to open multimedia channels. The endpoint must also support H.245 tunneling.

H.245 Tunneling uses Q.931 messaging for transporting H.245 messages. H.245 establishment messages (TCS, MSD, TCS Ack, MSD Ack) are encapsulated within Q.931 messages (Setup, Call Proceeding, Alerting, Connect). The H.245

establishment messages can be exchanged during Q.931 establishment. A tunneled H.245 Control call can be connected immediately after a Q.931 message is established. Each Q.931 message can contain any number of H.245 messages encoded into octet strings.

Note To enable H.245 tunneling the LifeSize Gatekeeper must be configured to operate in the **Call Setup (Q.931) and Call Control (H.245)** routing mode. For more information about routing modes, see Calls on page 50.

Third Party Call Control

Third Party Call Control enables administrators to:

- Connect and disconnect calls between two endpoints via the LifeSize Gatekeeper Administrator interface.
- Select and edit the parties to be dialed (using any kind of alias).
- Initiate a call from the LifeSize Gatekeeper.
- Disconnect a call from the LifeSize Gatekeeper.
- View call details for all third party-controlled calls in progress.

You configure Third Party Call Control via the **Make Call** dialog box in the **Call Control** tab. For more information about Third Party Call Control, see the Call Control Tab chapter.

Note To enable Third Party Call Control, the LifeSize Gatekeeper must be configured to operate in the **Call Setup (Q.931) and Call Control (H.245)** routing mode. For more information about routing modes, see Calls on page 50.

Predefined Endpoint Authentication by Alias

This feature enables you to specify the number of alias matches necessary for successful authentication and registration of predefined endpoints. For information about configuring alias matches, see Basics on page 46 and LDAP on page 71, and the Predefined Endpoint Authentication by Alias appendix.

Registration Restrictions

The **Registration Restrictions** tab enables you to view and configure registration restriction information. You can define rules for specifying the length of the E.164 alias, the alias prefix and the range of IP addresses with which the LifeSize Gatekeeper allows an endpoint to register. For more information on restricting user registration, see the Registration Restrictions Tab chapter.

RADIUS Server Support

The **Radius** section of the **Settings** tab enables LifeSize Gatekeeper support for a RADIUS (Remote Access Dial-In User Service) server for authentication, authorization and accounting. For information about configuring the LifeSize Gatekeeper to connect to a RADIUS server, see Radius on page 89.

External API Support

The **External API** section of the **Settings** tab enables LifeSize Gatekeeper support for communication via XML messages with external authorization servers and third party call control client applications. For more information, see External API on page 81.

Automatic Reset

Automatic reset enables the LifeSize Gatekeeper to catch service exception messages and to automatically reset the PC on which the LifeSize Gatekeeper runs. On automatic reset, LifeSize Gatekeeper logs are copied to a new folder and stored.

H.350 Standard Support

The LifeSize Gatekeeper supports the ITU-T H.350 standard for storing and retrieving video and voice over Internet Protocol (VoIP) information from enterprise directories. H.350 enables you to link account management and authorization automation to the enterprise directory using the Lightweight Directory Access Protocol (LDAP).

User Groups

The **Groups** section of the **Endpoints** tab enables you to define user groups for easy management of multiple endpoints. You can configure group member rules, permissions, allowed services and bandwidth settings for all members of the specified group. For more information, see Groups on page 140.

Bandwidth Policy

The **Bandwidth Policy** configuration tab also enables you to define rules for the management of bandwidth resources on your network.

Subzones

The **Bandwidth Policy** configuration tab enables you to define multiple subzones within the LifeSize Gatekeeper zone. You can define subzone rules, enabling bandwidth control within and between each subzone.

For information about configuring LifeSize Gatekeeper bandwidth management, see Bandwidth Policy on page 175.

IP Address Dialing Control

IP address dialing control enables you to instruct the LifeSize Gatekeeper when to block incoming calls dialed using an IP address only, with no alias. For more information, see Allow calls dialed with an IP address on page 53.

Advanced Call Fallback

The Call Fallback feature enables you to configure rules to deal with cases where:

- The LifeSize Gatekeeper cannot resolve a destination address in the IP network.
- The LifeSize Gatekeeper reaches the maximum bandwidth rate setting for any one of the configured endpoints, groups, subzones or zones.
- The LifeSize Gatekeeper receives an LRJ message from a Neighbor Gatekeeper because a destination endpoint cannot be located.
- The LifeSize Gatekeeper times out before receiving an LRJ message from Neighbor Gatekeeper because the timeout interval for an LRQ message has passed (for example, due to network failure).
- Resolution of a destination address fails for any other reason (for example, a call is to a disallowed service).

You can choose to route a call to an alternate H.323 alias address, to route the call to a service, to send calls through the local gateway or to reject a call. For more information about the Call Fallback feature, see Fallback on page 213.

ISDN Bypass

Check to forward calls over the ISDN network via a gateway.

When there is not enough bandwidth over the IP network to carry further calls, the LifeSize Gatekeeper can send a call through the local gateway for transmission over the ISDN network via a gateway. For information on configuring the ISDN Bypass feature, see ISDN bypass on page 217.

Caller ID Presentation Control

The caller ID presentation control feature enables the LifeSize Gatekeeper to control whether presentation of the caller ID to the receiving endpoint is allowed or restricted.

You enable the feature via the LifeSize Gatekeeper XML API or via configuration of the LDAP server.

- In the LifeSize Gatekeeper XML API, set the *RestrictCallerIdPresentation* field in the **Call Authorization Response** parameter to *Yes*.
- In the LDAP server, use the H.350 schema and define the *h323IdentityServiceLevel* attribute with either the *HideCallerId* or the *ShowCallerId* string.

In the LifeSize Gatekeeper, you enable or disable the feature for LDAP retrieval via the **Get Caller ID presentation policy** option in the **LDAP** section of the **Settings** tab.

When enabled, the LifeSize Gatekeeper verifies whether presentation of the caller ID to the receiving endpoint should be restricted or allowed. The LifeSize Gatekeeper makes a decision according to inputs from XML and LDAP, if such inputs exist. Before forwarding a call to the destination endpoint, the LifeSize Gatekeeper changes the value of the *presentationIndicator* field according to the inputs received in the Setup message from the source of the call.

The LifeSize Gatekeeper checks each the following inputs in turn in the specified order:

- The XML authorization response to the call.

  If the XML authorization response includes a caller ID presentation instruction, the LifeSize Gatekeeper allows or blocks presentation of the caller ID to the receiving endpoint according to this instruction.

  If the XML authorization response does not refer to caller ID presentation, the LifeSize Gatekeeper checks the LDAP server.

- The LDAP H.350 schema definition for the source endpoint.

  If the *h323IdentityServiceLevel* attribute contains either the *HideCallerId* string or the *ShowCallerId* string, the LifeSize Gatekeeper acts accordingly.

  If neither the *HideCallerId* string nor the *ShowCallerId* string is defined in the *h323IdentityServiceLevel* attribute for the source endpoint, the LifeSize Gatekeeper does not change the *presentationIndicator* field in the Setup message.

- The source endpoint request for presentation restriction in the Setup message.

  If there is no *presentationIndicator* field in the Setup message, the LifeSize Gatekeeper creates the field. If there are no other inputs from XML or LDAP, or if the **Get Caller ID presentation policy** option is unchecked, the LifeSize Gatekeeper uses a default value of presentation allowed.

When disabled, the LifeSize Gatekeeper does not change the *presentationIndicator* field. The indication in the source endpoint Setup message determines whether or not caller ID presentation is allowed.

2

GATEKEEPERS

WHAT'S IN THIS CHAPTER

The LifeSize Gatekeeper is an H.323 gatekeeper. This chapter introduces you to the following:

- H.323 Recommendation
- H.323 Gatekeepers

This chapter is optional and has been provided to give a better understanding of what H.323 gatekeepers are. This knowledge is not essential for working with the LifeSize Gatekeeper but it may assist you in making better decisions when configuring the LifeSize Gatekeeper. Therefore, you should read this chapter if you are not familiar with H.323 gatekeepers or you wish to make the most of LifeSize Gatekeeper functionality.

H.323 RECOMMENDATION

H.323 is an umbrella recommendation of the International Telecommunications Union (ITU-T) that specifies the complete architecture and operation of real-time multimedia communications over packet networks. H.323 is very broad in scope, including both stand-alone devices and embedded personal computer technology. It defines models of interaction for both endpoint-to-endpoint and multipoint conferences.

In the document that details Recommendation H.323, references are made to other standards including *H.225.0* and *H.245*. H.225.0 specifies the procedures and messages applicable to gatekeepers, including the *RAS* protocol for Registration, Admission and Status. H.225.0 also includes the *Q.931* protocol for Call Signaling, consisting of Setup, Teardown and Disengage. H.225.0 also refers to H.245.

H.245 provides signaling for the proper operation of the H.323 terminal, including capabilities exchange, opening and closing of logical channels together with a full description of these channels, mode preference requests, flow control messages, and general commands and indications. H.245 signaling is established between two endpoints, an endpoint and an LifeSize Multipoint, or an endpoint and a gatekeeper. For each call in which the endpoint participates, the endpoint establishes exactly one H.245 Control channel. This channel uses the messages and procedures of Recommendation H.245.

All messages that are exchanged between two or more H.323 entities use the Abstract Syntax Notation One (ASN.1) language. ASN.1 is a language for describing the complex data structures independently from the underlying hardware. ASN.1 is a standard developed by the ITU-T and is described in Recommendations X.680-X.694.

H.323 GATEKEEPERS

A gatekeeper is at the heart of the H.323 network. Gatekeepers manage the H.323 entities that are capable of receiving or initiating calls. These entities—terminals, gateways and multiple control units (LifeSize Multipoints)—are called *endpoints*.

Each gatekeeper has a zone. An endpoint that registers with a gatekeeper becomes part of the zone of that gatekeeper. The main function of the gatekeeper within its zone is to provide call control services for its endpoints. Gatekeeper functions include:

- Address resolution, by translating IP network aliases for endpoints into transport addresses.
- Admissions control for authorizing network access.
- Bandwidth management.
- Network management (in Routed Mode).

The LifeSize Gatekeeper supports all the mandatory requirements stated in H.323. The LifeSize Gatekeeper also supports additional functions necessary for effective advanced
audio/video conferencing in networks.

Gatekeeper Procedures

The H.323 Recommendation specifies *procedures* that define the standard operational characteristics and behavior of a gatekeeper in a network. These procedures describe the steps needed to fulfill a policy or provide a service. *Messages* enable the procedures to accomplish what the policies or services need to do. The LifeSize Gatekeeper implements standard H.323 gatekeeper procedures according to the specification of the RAS and the Call Signaling protocols.

The H.323 Recommendation also states that certain functionality can be built into a gatekeeper, based on standard gatekeeper procedures. Policies that are built into the LifeSize Gatekeeper provide the basic framework for fundamental gatekeeper behavior and also establish Default Policies for certain procedures, such as how to control a zone.

Call Establishment

Calls are established on the RAS channel, which is the unreliable (UDP) channel for Registration, Admission and Status messages, as described below.

Gatekeeper Discovery

Call establishment often starts with Gatekeeper Discovery, which is an automatic procedure that occurs before a conference starts. In Gatekeeper Discovery, an endpoint looks for a gatekeeper with which to register by multicasting a Gatekeeper Discovery Request message (GRQ). Upon receiving a GRQ message, the gatekeeper either returns a Gatekeeper Confirm message (GCF) with the transport address of the RAS channel of the gatekeeper, or if the gatekeeper does not want the endpoint to register with it, the gatekeeper returns a Gatekeeper Reject message (GRJ).

Gatekeeper Discovery allows the endpoint-gatekeeper association to change over time. The advantage of this procedure is two-fold:

- Administrative overhead is lower, since there is no need to configure individual endpoints.
- An existing gatekeeper can be replaced without the need to manually reconfigure all of the affected endpoints.

The gatekeeper does not maintain an internal database based on the Discovery procedure since the requesting endpoint is not obliged to register with this specific gatekeeper at a later time.

Note Gatekeeper Discovery is not mandatory. If a gatekeeper IP address is preconfigured in the endpoint, Gatekeeper Discovery does not occur.

Gatekeeper Registration

After discovering gatekeepers, both endpoints then register with a gatekeeper using the Registration Request message (RRQ). In this process each endpoint joins a *zone* and informs the gatekeeper of its transport and alias addresses, such as names or phone numbers. Registration occurs before any calls are attempted and may occur periodically, or once, such as during endpoint power-up.

The gatekeeper is capable of receiving registrations from endpoints with multiple transport addresses, such as gateways or LifeSize Multipoints. Upon receiving an RRQ message from an endpoint, the gatekeeper responds with either a Registration Confirm message (RCF) or a Registration Reject message (RRJ).

Location Request

An endpoint or gatekeeper can request the location of another endpoint using its alias name by sending a Location Request message (LRQ), and the gatekeeper replies with a Location Confirm message (LCF) containing the resolved address for the alias name.

Admission Request

When a user places a call from an endpoint, the endpoint starts by requesting admission from the gatekeeper using an Admission Request message (ARQ). The gatekeeper can accept by sending an Admission Confirm message (ACF), or deny the request by sending an Admission Reject message (ARJ). If the call is accepted, the endpoint sends a Q.931 Setup message to the remote party. The remote party that receives the Setup message then requests admission from its gatekeeper by sending an ARQ. If the call is accepted, the Q.931 Call Signaling process is completed when, in the Q.931 Connect message, an endpoint receives a reliable transport address to which to send the control messages. H.245 message negotiation then follows. It is at this stage that an endpoint can request additional bandwidth by sending a Bandwidth Request message (BRQ) to its gatekeeper.

Routing H.225.0 Call Signaling Channels

The Call Signaling channel is a reliable TCP channel for carrying H.225.0 Call Signalling messages, as discussed above. This section discusses the methods for passing Call Signaling messages between two endpoints.

Routed and Direct Modes

The two methods for passing Call Signaling messages between two endpoints are:

- *Direct Mode* which passes Call Signaling messages directly between two endpoints.
- *Routed Mode* which routes Call Signaling messages, and possibly H.245 messages, between two endpoints via the gatekeeper.

During the initial Admission Procedure, a parameter in the ACF message specifies the mode in which the gatekeeper should be set for the specific requested call. The Default Policy for all calls, excluding calls to a supported prefix of a gateway, can be defined by the gatekeeper administrator using the zone properties configuration.

DIRECT MODE FLOW

Figure 2-1 shows the flow of RAS and Call Signaling messages in Direct Mode.

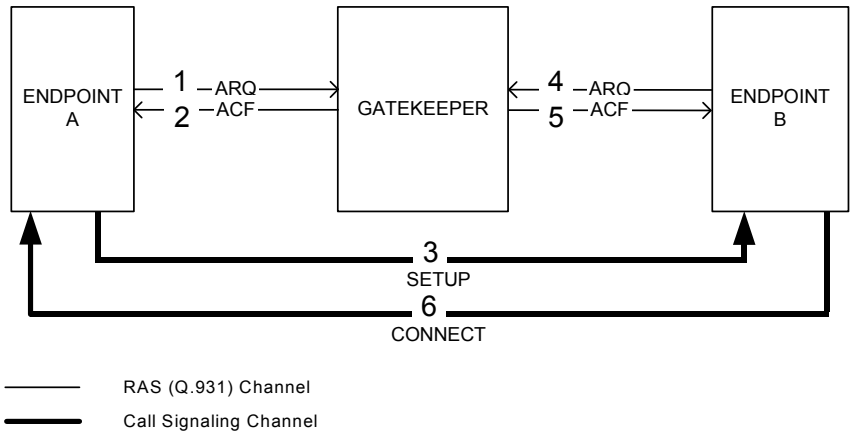

Figure 2-1 *Direct Call Signaling*

ROUTED MODE FLOW

Figure 2-2 shows the flow of RAS and Call Signaling messages in Routed Mode. In this case, the gatekeeper keeps the Call Signaling channel open while routing the call for the duration of the call. The H.245 Control channel is established directly between the two endpoints.

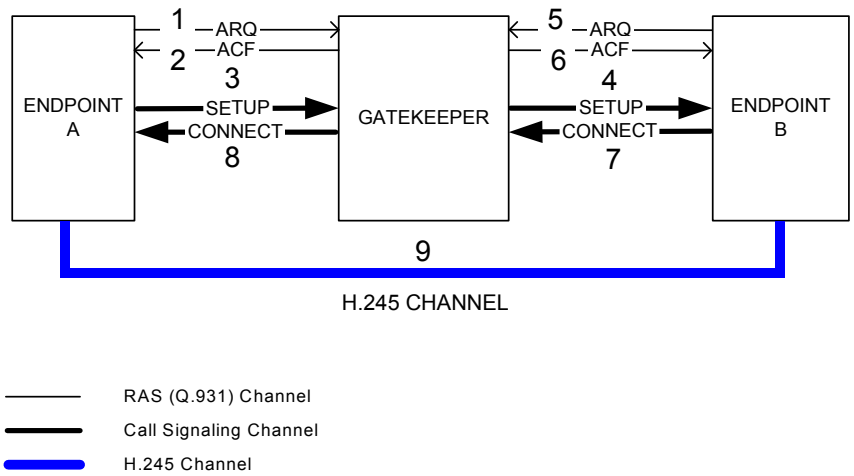

Figure 2-2 *Routed Call Signaling*

Routing H.245 Control Channels

In addition to the Call Signal routing mode, the gatekeeper can route H.245 Control channels. To establish a H.245 routed call, the gatekeeper administrator can define an H.245 routed mode as a Default Policy for all calls. Figure 2-3 shows H.245 routed Call Signaling.

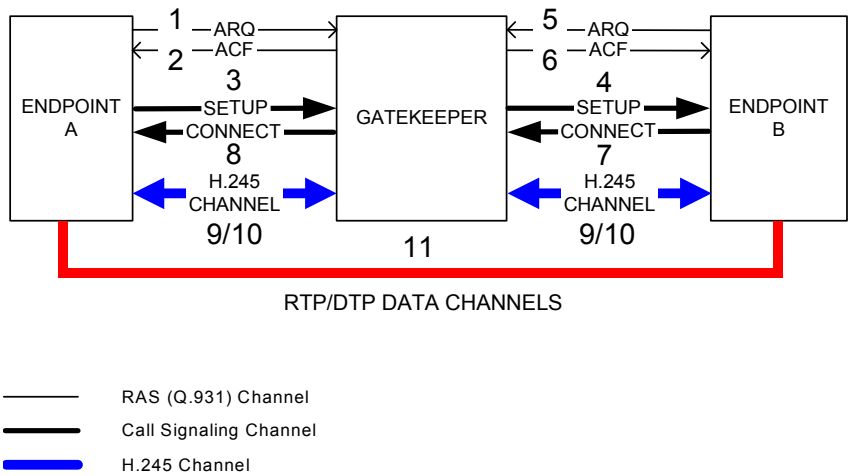

Figure 2-3 *H.245 Routed Call Signaling*

Call Termination

A call can be terminated in a number of ways, as described below.

Disengage Request

To terminate a call, both endpoints send a Disengage Request message (DRQ) to inform the gatekeeper that a call is being terminated. The gatekeeper can accept or reject this request.

Unregistration Request

An alternative to a Disengage Request message is an Unregistration Request message (URQ). Either an endpoint or a gatekeeper can unregister an endpoint.

Endpoint-Initiated Unregistration

When the gatekeeper receives a URQ message from a valid endpoint, the gatekeeper views the request details and can either accept or reject the request.

Gatekeeper-Initiated Unregistration

The gatekeeper uses the H.323 polling mechanism (IRQ/IRR), or the Time To Live message (TTL) sent by the endpoint, for detecting endpoints that went offline without performing Unregistration. When the gatekeeper detects that an endpoint is not active, the gatekeeper initiates a URQ message.

Support of Endpoints without RAS Capabilities

The gatekeeper partially supports endpoints that do not support RAS. You can predefine aliases for these endpoints with the gatekeeper. The gatekeeper stores these aliases as dynamic data and thus can route calls to these endpoints.

The gatekeeper also gives services to calls from endpoints that do not support RAS, by relating to these calls as out-of-zone calls. In this case, the gatekeeper does not give the endpoint predefined permission to services or predefined distances, and it does not forward calls to the endpoint. However, the gatekeeper allows these endpoints to access services defined as public for out-of-zone endpoints.

Configuring the LifeSize Gatekeeper

3

WORKING WITH THE LIFESIZE GATEKEEPER

WHAT'S IN THIS CHAPTER

This chapter introduces you to the following:

- Introducing the Web Interface
- Accessing the Web Interface
- Login Profiles
- Configuration Interface
- Global Configuration Tabs
- LifeSize Gatekeeper Configuration Tabs

INTRODUCING THE WEB INTERFACE

The LifeSize Gatekeeper Administrator is a web interface that enables you to configure any element of the LifeSize Gatekeeper through a single point of entry.

Access to the configuration interface is controlled by a user name and a password. Once you have entered the settings you want, you can upload them to the LifeSize Gatekeeper database or save them to a configuration file to be loaded at a later time.

REQUIREMENTS FOR THE WEB INTERFACE

To use the LifeSize Gatekeeper Administrator web interface you require the following:

- A Java-compliant web browser. Microsoft Internet Explorer version 5.5 or later is recommended.

ACCESSING THE WEB INTERFACE

You access the LifeSize Gatekeeper Administrator web interface using the **Product Family Entry Point** web interface. The **Product Family Entry Point** web interface provides a comprehensive list of network devices currently available with active links to the web interface of each device. The **Product Family Entry Point** list includes information about each device including IP address, product type, version and icons which indicate the device type. You can sort the order of the list by clicking on any of the list headings with which you wish to sort the list.

You access the LifeSize Gatekeeper Administrator web interface for a specific LifeSize Gatekeeper simply by clicking on the IP address of the LifeSize Gatekeeper you wish to manage. A separate window is opened to display the web interface of the LifeSize Gatekeeper you selected. You can return to the main list at all times to access and manage other devices.

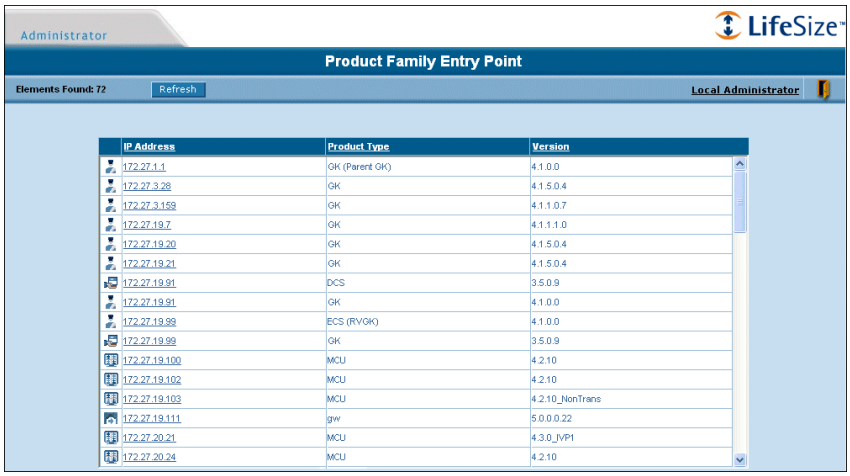

Figure 3-1 *Product Family Entry Point Interface*

To access the LifeSize Gatekeeper Administrator configuration interface

1. In your browser, enter the name of the device on which the LifeSize Gatekeeper resides.

   Press **Enter** to display the **Login** screen (Figure 3-2).

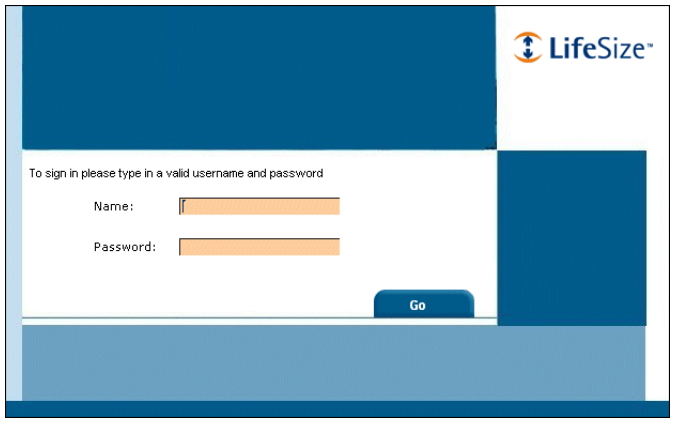

Figure 3-2 *LifeSize Gatekeeper Administrator Login Screen*

2. Enter your user name and password and click **OK** to proceed to the **Product Family Entry Point** web interface. The default user name is *admin* and the default password is null.

   The **Product Family Entry Point** interface displays.

3. Click the IP address of the device you wish to manage or click **Local Administrator** to access the LifeSize Gatekeeper Administrator configuration interface.

   Clicking the IP address opens the **Login** screen again.

4. Enter your user name and password and click **OK**.

   The LifeSize Gatekeeper Administrator configuration interface displays (Figure 3-3).

LOGIN PROFILES

You can log in to the LifeSize Gatekeeper as

- An **administrator**—Administrators have access to all LifeSize Gatekeeper configuration options.
- An **operator**—Operators can view all LifeSize Gatekeeper configuration options, but can modify only the **Make Call** function in the **Call Control** tab. For more information, see Enabling Third Party Call Control on page 197.
- A **guest**—Guests can view the **Endpoints** tab only, and cannot modify any LifeSize Gatekeeper configuration settings.
- A **read-only** user—Read-only users can view all LifeSize Gatekeeper configuration options, but cannot modify any LifeSize Gatekeeper configuration settings.

Note If you try to log in as an **Administrator** in the **Login** screen and another **Administrator** is currently logged in, the LifeSize Gatekeeper logs you in as a **Read only** user and the words **Read Only** appear above the toolbar. **Read only** users cannot modify any of the LifeSize Gatekeeper settings.

CONFIGURATION INTERFACE

The LifeSize Gatekeeper Administrator configuration interface consists of a sidebar, a horizontal toolbar and configuration tabs in the main frame of the screen.

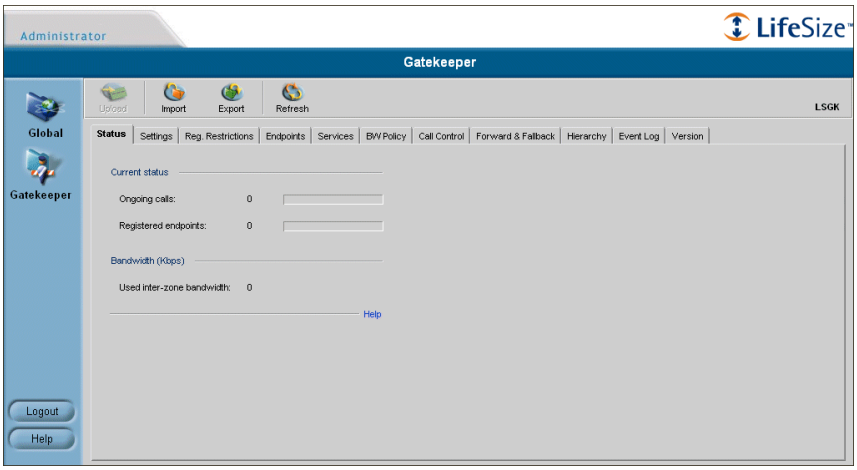

Figure 3-3 *Gatekeeper Configuration Administrator Interface*

SIDEBAR

The sidebar enables you to navigate between the different configuration interfaces. The following navigation buttons are available:

- **Global**

  Displays user information and host server application information. For more information about the Global interface, see Global Configuration Tabs on page 38.

- **Gatekeeper**

  Displays the LifeSize Gatekeeper configuration interface.

- **Logout**

  Enables you to log out of the current LifeSize Gatekeeper configuration session.

Note You may be logged out automatically if the LifeSize Gatekeeper Administrator is inactive for approximately five minutes.

- **Help**

  Displays the Help contents page for the element in the sidebar that you have selected. Clicking **Help** on any individual tab accesses the Help Contents for that tab alone.

  You can also access the LifeSize Gatekeeper online help via a shortcut in the **Start** menu of your computer. The path is:

  Start > Programs > LifeSize > LifeSize Gatekeeper > LifeSize Gatekeeper Help

TOOLBAR

The LifeSize Gatekeeper Administrator toolbar consists of the following buttons, displayed according to the version of the LifeSize Gatekeeper and the element you select (Global or Gatekeeper):

Table 3-1 *Global and LifeSize Gatekeeper Toolbar Commands*

Button	Description	Global	Gatekeeper
Upload	Sends the defined configuration parameters from the LifeSize Gatekeeper Administrator interface to the LifeSize Gatekeeper. The **Upload** button is enabled only after you configure any of the fields in the tab currently displayed.	●	●
Import	Loads a saved LifeSize Gatekeeper configuration file from a directory on your PC or from the IP network to the LifeSize Gatekeeper Administrator interface. Click **Upload** to apply the settings to the LifeSize Gatekeeper.	–	●
Export	Saves the LifeSize Gatekeeper configuration information to a file on the computer. You set the file name during the save process.	–	●
Refresh	Retrieves current configuration parameters from the LifeSize Gatekeeper and displays them in the LifeSize Gatekeeper Administrator interface.	●	●

GATEKEEPER IDENTIFIER INDICATION

A Gatekeeper identifier indication appears on the right side of the toolbar. The Gatekeeper identifier is the same as the name that you enter in the **Gatekeeper ID** field in the **Basics** section of the **Settings** tab. The Gatekeeper identifier used in the screens throughout this manual is LS**GK**.

Global Configuration Tabs

The Global configuration is grouped into the following tabs:

- Users Tab
- Applications Tab

Users Tab

The Global **Users** tab enables you to create and modify the user names, access level groups and passwords of the users authorized to use the LifeSize Gatekeeper.

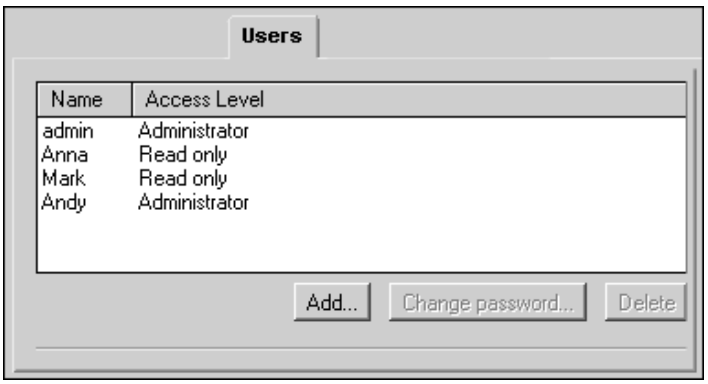

Figure 3-4 *Global Users Tab*

What You Can See

The following information is displayed in the **Users** tab:

Table 3-2 *Users Tab Configuration*

Field	Description
Name	Displays the user name of the specified user.
Access Level	Displays the access level for the specified user.

What You Can Configure

The following options are available in the **Users** tab:

Add

Displays the **Add User** dialog box for defining new user profiles.

Change password

Displays the **Change Password** dialog box for modifying a user password.

Delete

Deletes the specified user entry.

Adding or Modifying a User Profile

Select a user from the **Users** tab and click the **Add** button to open the **Add User** dialog box for adding new users to the LifeSize Gatekeeper database, or click the **Change password** button to open the **Change Password** dialog box for changing the password of the specified user.

The following options are available in the **Add User** and **Change Password** dialog boxes:

User name

Enables you to type the name of the user or displays the name of the user.

Access Level

Enables you to select the access level for the user or displays the access level. The access level defines the specific rights granted to the user.

Password

Type a password for the user. The password is case-sensitive.

Confirm password

Re-enter the password for the user.

Upload

Click the **Upload** button to add the user information to the LifeSize Gatekeeper database.

APPLICATIONS TAB

The Global **Applications** tab displays a list of the LifeSize server applications running on the LifeSize Gatekeeper host computer. You can start or stop a selected application.

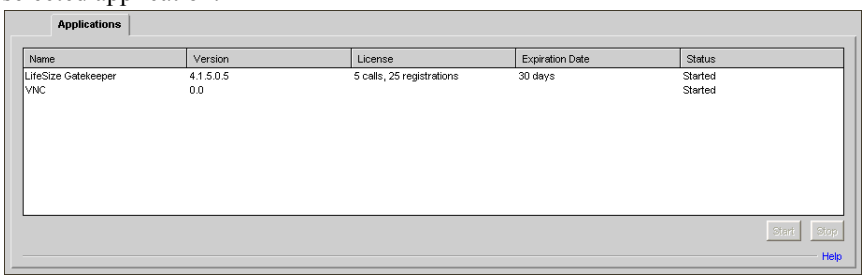

Figure 3-5 *Global Applications Tab*

WHAT YOU CAN SEE

The following information is displayed in the **Applications** tab:

Table 3-3 *Applications Tab Configuration*

Field	Description
Name	Displays the name of the application.
Version	Displays the application software version number.
License	Displays the licensing information for the application.
Expiration Date	Displays expiration date information for the application.
Status	Displays the operational status of the application.

WHAT YOU CAN CONFIGURE

The following options are available in the **Applications** tab:

Start

Click to start the operation of a specified application.

Stop

Click to stop the operation of a specified application.

LifeSize Gatekeeper Configuration Tabs

The LifeSize Gatekeeper configuration information is grouped into the following tabs:

- **Status**

  Enables you to view the total number of current calls and current registrations, and the total bandwidth currently in use.

- **Settings**

  Enables you to define the mode of operation of the LifeSize Gatekeeper.

- **Registration Restrictions**

  Enables you to define rules for specifying the length of the E.164 alias, the alias prefix and the range of IP addresses with which the LifeSize Gatekeeper allows an endpoint to register.

- **Endpoints**

  Enables you to view a list of all currently registered endpoints and their basic parameters and to add, modify and delete predefined endpoint properties. Enables you to configure and view group settings, and to add endpoints to groups or delete endpoints from groups. You can also unregister selected or all endpoints.

- **Services**

  Enables you to view, add and modify the services provided by the LifeSize Gatekeeper.

- **BW Policy**

  Enables you to define subzones and subzone rules, and to determine bandwidth policy between zones and subzones.

- **Call Control**

  Enables you to monitor current calls, view call details and disconnect calls.

- **Forward & Fallback**

  Enables you to view and configure Call Forwarding and Call Fallback rules.

- **Neighbors**

  Enables you to view, configure and modify Neighbor Gatekeepers and their IP addresses.

- **Hierarchy**

  Enables you to view, configure and modify a hierarchy of gatekeepers. Replaces the **Neighbors** tab when the **Dial Plan** field in the **Basics** section of the **Settings** tab is set to **Version 2**.

- **Event Log**

  Enables you to monitor LifeSize Gatekeeper alarm events.

- **Security Passwords**

  Enables you to view, configure and modify user names and passwords for endpoints that are registered with the LifeSize Gatekeeper. Appears only when you enable H.235 security in the **Security** section of the **Settings** tab.

- **Version**

  Enables you to view the version numbers of the various system components.

Note Global and Gatekeeper settings must be uploaded separately since settings you have entered are not saved when you move from the Global interface to the Gatekeeper interface, and from the Gatekeeper interface to the Global interface.

4

STATUS TAB

ABOUT THE STATUS TAB

The **Status** tab displays the total number of current calls and registrations, and the total bandwidth used. The network administrator uses this tab to monitor the current call, registration and bandwidth usage at any point in time.

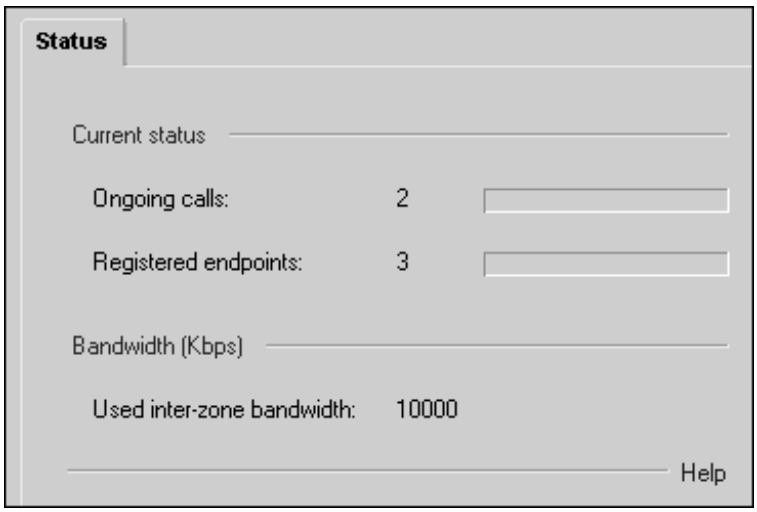

Figure 4-1 *Status Tab*

What You See

The following information is displayed in the **Status** tab:

Current Status

Ongoing calls

Displays the number of calls currently in the LifeSize Gatekeeper.

Registered endpoints

Displays the number of endpoints currently registered in the LifeSize Gatekeeper.

Bandwidth (Kbps)

Used inter-zone bandwidth

Displays the total bandwidth currently in use for calls from the zone to an out-of-zone destination, and for calls entering the zone from an out-of-zone source.

5

SETTINGS TAB

ABOUT THE SETTINGS TAB

The **Settings** tab enables you to configure the LifeSize Gatekeeper to suit your environment and requirements. You define the mode of operation of the LifeSize Gatekeeper by specifying registration and address resolution policies, routing options, bandwidth usage and other capacity characteristics, H.450 Supplementary Services parameters, logging options, LifeSize Gatekeeper identifier name and other parameters. Even before you specify your own preferences, the LifeSize Gatekeeper can begin to accept registrations and calls using its default settings.

Note If you wish to modify the settings, it is advisable to do so immediately after starting the LifeSize Gatekeeper. When you are in an active LifeSize Gatekeeper session, it is not advisable to change the Dynamic IP policy or the LifeSize Gatekeeper identifier. If you need to change either of these values, you must stop the LifeSize Gatekeeper, restart it and immediately make the changes before accepting registrations or calls.

You specify these parameters in the following sections of the **Settings** tab, which are described in detail below.

- Basics
- Calls
- Capacity
- Dial Plan
- Supplementary Services

- Logs
- Billing
- Alert Indications
- LDAP
- External API
- DNS
- Central Database
- Radius
- Security
- Alternate Gatekeeper
- Advanced

BASICS

The **Basics** section of the **Settings** tab enables you to define LifeSize Gatekeeper registration policy.

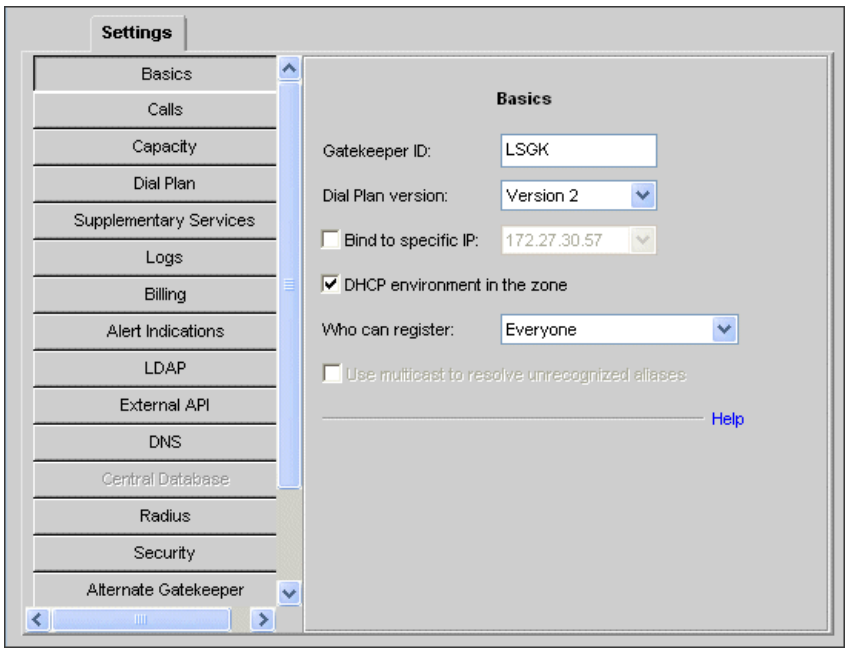

Figure 5-1 *Settings Tab: Basics*

WHAT YOU CAN CONFIGURE

The following options are available for configuring basic LifeSize Gatekeeper policies:

Gatekeeper ID

Enter the LifeSize Gatekeeper identifier name. You can use any combination of characters and/or digits up to a maximum of 64. If you are using LDAP:

- The LifeSize Gatekeeper identifier must be unique for each LifeSize Gatekeeper.
- The LifeSize Gatekeeper identifier must be the same as the name you enter in the **Full name** field in the LDAP Online Information Tree.

For more information, see Modifying the LDAP Tree on page 254.

Dial Plan version

Select the version of the Dial Plan you want to use. The default setting is **Version 2**. **Version 2** enables the **Dial Plan** section of the **Settings** tab, opens the **Services** and **Global Services** sections in the **Services** tab and replaces the **Neighbors** tab with the **Hierarchy** tab. For more information about the Dial Plan, see Dial Plan on page 57 and the LifeSize Gatekeeper Dial Plan version 2 appendix.

Note Selecting Dial Plan version 1 disables the **Dial Plan** section of the **Settings** tab and prevents you accessing the hierarchy information configured in the **Dial Plan** section. You can access this information by selecting **Version 2** in the **Dial Plan version** field.

Bind to specific IP

Check to enable the LifeSize Gatekeeper to bind to a specific NIC card on the host computer, where the host contains more than one NIC card. Specify the IP address of the required NIC card in the adjacent field.

Note When working with two NIC cards in your server, do not disable the IP address belonging to the NIC used for generating the license key.

DHCP environment in the zone

Select this option to instruct the LifeSize Gatekeeper to refer to the network as a Dynamic Host Configuration Protocol (DHCP) environment. In this environment, IP Policy is dynamic.

The LifeSize Gatekeeper uses some of the predefined information as management keys to identify endpoints. These keys are the alias name or phone numbers in a DHCP environment. A terminal does not have a constant IP in a DHCP environment. DHCP operation mode supports user mobility between workstations.

In a non-DHCP environment, the management key is the IP address. The main keys for registering an endpoint are the registration IP, terminal alias and endpoint type.

You can configure the LifeSize Gatekeeper to complete partial information. When an endpoint registers with the LifeSize Gatekeeper using partial information, such as the registration IP address and terminal alias without a phone number, the LifeSize Gatekeeper supplies the missing information to the endpoint.

Who can register

Available only if the LifeSize Gatekeeper is licensed to receive registrations. Select the LifeSize Gatekeeper registration policy from the following options in the drop-down list:

- **Everyone** sets an open zone policy that allows the LifeSize Gatekeeper to accept any legal registrations from any endpoint. This is useful for enabling the LifeSize Gatekeeper to operate in a “plug-and-play” mode.
- **Only predefined endpoints** sets a strict zone policy where the LifeSize Gatekeeper only accepts registration from predefined endpoints. This provides tighter control over the usage of network resources and services.
- **No endpoints** sets a closed zone policy that prevents the LifeSize Gatekeeper from accepting any registration. This is useful for the orderly shutdown of the LifeSize Gatekeeper.

Note You can also configure endpoints and carry out the authentication process in the LDAP server. For more information, see the Configuring the LDAP Server chapter.

Number of aliases to authenticate in DHCP environment

Type the maximum number of alias matches that must be successfully made for an endpoint to be able to register to the LifeSize Gatekeeper in DHCP operation mode. For example, if you set this field to 4 and an endpoint is predefined with 3 aliases, the endpoint must match at least 3 aliases. The default setting and the minimum allowed setting is 1.

The LifeSize Gatekeeper attempts to match an endpoint alias with the list of predefined endpoint aliases in the LifeSize Gatekeeper database. For more information about DHCP, see DHCP environment in the zone on page 48. For more information about configuring this option, see the Predefined Endpoint Authentication by Alias appendix.

Note The **Number of aliases to authenticate in DHCP environment** option is enabled only when the **DHCP environment in the zone** option is checked, and when **Only predefined endpoints** is selected in the **Who can register** field.

Number of aliases to authenticate in non-DHCP environment

Type the maximum number of alias matches that must be successfully made for an endpoint to be able to register to the LifeSize Gatekeeper in non-DHCP operation mode. For example, if you set this field to 4 and an endpoint is predefined with 3 aliases, the endpoint must match at least 3 aliases. The default setting and the minimum allowed setting is 0.

Note When this field is set to 0, endpoint authentication is performed according to IP address only.

The LifeSize Gatekeeper attempts to match an endpoint alias with the list of predefined endpoint aliases in the LifeSize Gatekeeper database. For more information about DHCP, see DHCP environment in the zone on page 48. For more information about configuring this option, see the Predefined Endpoint Authentication by Alias appendix.

Note The **Number of aliases to authenticate in non-DHCP environment** option is enabled only when the **DHCP environment in the zone** option is unchecked, and when **Only predefined endpoints** is selected in the **Who can register** field.

Use multicast to resolve unrecognized aliases

When checked, instructs the LifeSize Gatekeeper to resolve unrecognized aliases by using multicast to send a Location Request message (LRQ) to other gatekeepers. This may be in addition to using unicast. This option is disabled when **Version 2** is selected in the **Dial Plan version** field. For more information about the LRQ policy of the LifeSize Gatekeeper, see Resolution of Aliases on page 9.

Note Selecting the **Use multicast to resolve unrecognized aliases** option may result in heavy traffic on the IP network due to multicast messages.

CALLS

The **Calls** section of the **Settings** tab enables you to define various call options including call routing modes with or without the H.245 Proxy.

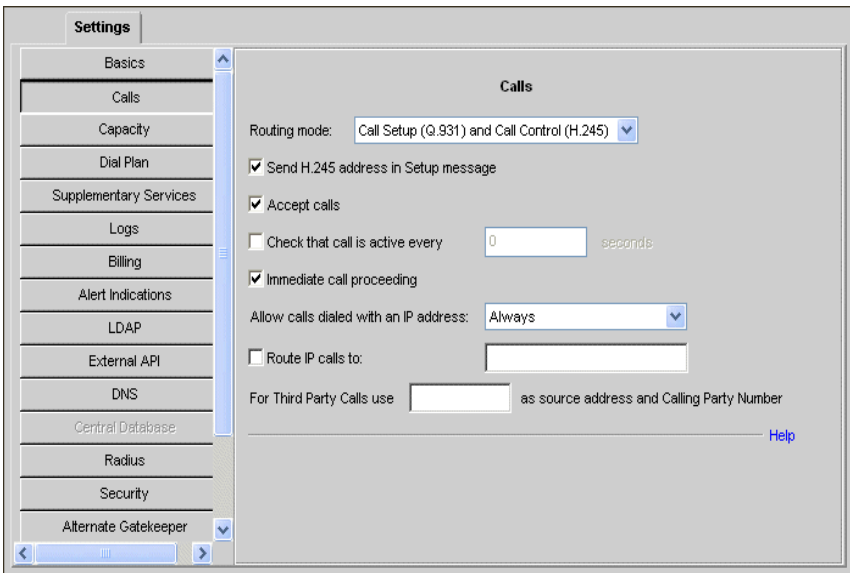

Figure 5-2 *Settings Tab: Calls*

About the H.245 Proxy

The H.245 Proxy enables routing of H.245 channels in a point-to-point H.323 call. When the H.245 Proxy is enabled (i.e. when you select the **Call Setup (Q.931) and Call Control (H.245)** option in the **Routing mode** field), the LifeSize Gatekeeper acts as a middleman between two endpoints for handling the H.245 channels. The Proxy allows the LifeSize Gatekeeper to:

- Control and monitor basic H.245 procedures.
- Control and monitor logical channel setup.
- Support Call Transfer as defined by Recommendation H.450.2.

What You Can Configure

The following options are available for configuring the **Calls** section:

Routing mode

Select **Direct** to route calls directly without LifeSize Gatekeeper intervention, **Call Setup (Q.931)** to route the Call Setup channel through the LifeSize Gatekeeper, or **Call Setup (Q.931) and Call Control (H.245)** to enable the H.245 Proxy to route the Call Setup channel and the Control channel through the LifeSize Gatekeeper. When you modify the routing mode you should manually update the routing mode setting on the LDAP server.

Note Direct call mode forms a connection directly between the Setup and Control channels of two endpoints. In this mode the LifeSize Gatekeeper does not provide call control functions for regular calls. *Regular* calls are calls which are not made to services (such as a gateway or LifeSize Multipoint). Direct call mode uses fewer LifeSize Gatekeeper resources.

Warning You must disconnect all calls before modifying the routing mode.

The following features work only in the **Call Setup (Q.931) and Call Control (H.245)** routing mode. For more information, see the LifeSize Gatekeeper Overview chapter.

- Third Party Call Control—For more information, see Third Party Call Control on page 14 and the Call Control Tab chapter.

Send H.245 address in Setup message

Select this option to include the H.245 address allocated by the H.245 Proxy in the outgoing Setup message. Selecting this option enables H.245 channels to connect before the call is actually connected. The **Send H.245 address in Setup message** field is enabled only when the **Call Setup (Q.931) and Call Control (H.245)** option is selected in the **Routing mode** field.

Accept calls

Select this option to enable the LifeSize Gatekeeper to accept calls. Clear the checkbox to prevent the LifeSize Gatekeeper accepting calls. This option is useful for orderly LifeSize Gatekeeper shutdown.

Check that call is active every *n* seconds

Check to enable the LifeSize Gatekeeper to identify calls which are no longer ongoing. The LifeSize Gatekeeper uses the H.323 polling mechanism which works with Information Request/Information Request Response (IRQ/IRR) messages. Enter an IRQ interval value in seconds to control the frequency with which the LifeSize Gatekeeper sends an IRQ message to check whether or not an endpoint is participating in a current LifeSize Gatekeeper session.

Warning Endpoints which do not support IRQ/IRR messages will not respond to H.323 polling. In such cases, the LifeSize Gatekeeper will disconnect calls.

Note The **Check that call is active every *n* seconds** option is enabled only when the **Routing mode** field is set to **Direct**.

The LifeSize Gatekeeper checks the activity of all endpoints listed as *On Call* in the **Endpoints** section of the **Endpoints** tab. For more information, see Endpoints on page 127. For more information about IRQ messages, see Advanced on page 104.

Immediate call proceeding

Select this option to enable the immediate sending of a Call Proceeding message by the LifeSize Gatekeeper during Call Setup for calls that are routed via the LifeSize Gatekeeper. Otherwise, the LifeSize Gatekeeper sends the Call Proceeding message only after the Call Proceeding message arrives from the destination endpoint.

Allow calls dialed with an IP address

Select an option from the drop-down list to instruct the LifeSize Gatekeeper when to block incoming calls dialed using an IP address only, with no alias.

Route IP calls to

Enter the IP address of a RADVISION PathFinder Server for firewall traversal. The LifeSize Gatekeeper forwards the call to the PathFinder Server with the original dialed IP as part of the destination list.

Disabled when **Allow calls dialed with an IP address** is set to **Never**.

For Third Party Calls use ... as source address and Calling Party Number

Enter the Fixed Calling Party Number alias for calls initiated by the LifeSize Gatekeeper. The alias will appear as the LifeSize Gatekeeper Fixed Calling Party Number in the CDR.

For more information about the Fixed Calling Party Number feature, see Fixed Calling Party Number on page 13, Configuring a Fixed Calling Party Number Alias on page 53 and Adding or Modifying a Predefined Endpoint on page 130.

Configuring a Fixed Calling Party Number Alias

Prerequisites

- The LifeSize Gatekeeper must be configured to operate in the **Call Setup (Q.931)** or **Call Setup (Q.931) and Call Control (H.245)** routing modes.

  For more information on routing modes, see Routing mode on page 51.
- For calls to a gateway, the endpoint alias must be the CPN.

To enable the Fixed Calling Party Number feature

Check the **Enable using a fixed Calling Party Number** field in the **Advanced** section of the **Settings** tab.

The **Use as Calling Party Number** indicator appears in the **Predefined Endpoint Properties** dialog box in the **Endpoints** section of the **Endpoints** tab (see Adding or Modifying a Predefined Endpoint on page 130).

Note The *CallingPartyNumber* and *SourceAddress* field values in the outgoing Setup message will be different. The H.323 standard requires them to be identical.

To create a new Fixed Calling Party Number alias

1. Click **Add** in the **Predefined Endpoint Properties** dialog box in the **Endpoints** section of the **Endpoints** tab.
2. Enter the alias name and select **Phone number** or **Party number** from the drop-down list in the **Type** field.

   The **Add Alias** dialog box displays.
3. Check the **Always use as Calling Party Number** option and click **OK**.
4. Click **Upload** in the **Predefined Endpoint Properties** dialog box.

   The selected alias appears in the **Aliases** section of the **Predefined Endpoint Properties** dialog box marked with an asterisk in brackets—[*]. The selected alias also appears in the *CallingPartyNumber* field of the outgoing Setup message.

Note The **Always use as Calling Party Number** field is enabled only when you select **Phone number** or **Party number** from the drop-down list in the **Type** field.

To change an existing alias into a Fixed Calling Party Number alias

1. Select the required alias from the **Aliases** section of the **Predefined Endpoint Properties** dialog box and click **Edit**.

   The **Edit Alias** dialog box displays.
2. Follow steps 2-4 of the To create a new Fixed Calling Party Number alias section.

CAPACITY

The **Capacity** section of the **Settings** tab enables you to define the bandwidth usage and other capacity characteristics of the LifeSize Gatekeeper.

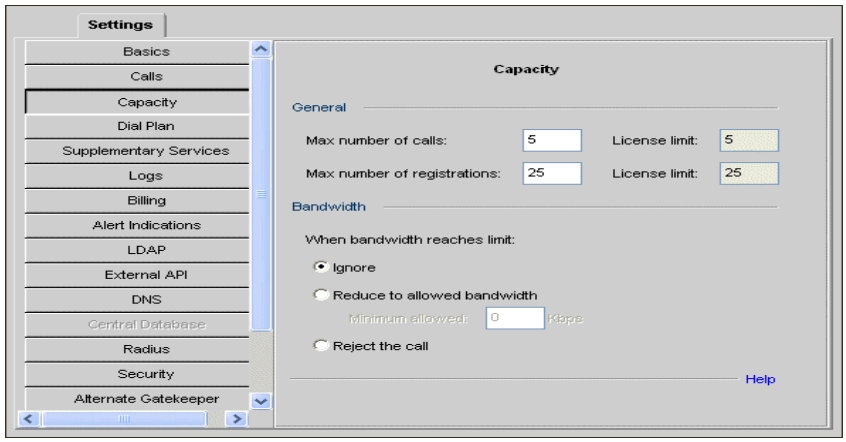

Figure 5-3 *Settings Tab: Capacity*

WHAT YOU CAN CONFIGURE

The following options are available for configuring the **Capacity** section:

GENERAL

Max number of calls

Enter the maximum number of calls allowed in the LifeSize Gatekeeper zone simultaneously. Use this parameter to regulate traffic by allowing more or less voice or videoconferencing on the network. The maximum number of calls allowed is shown on your license. The value shown on your license is the default setting.

License limit

Displays the maximum number of calls that your license allows.

Max number of registrations

Enter the maximum number of registrations allowed in the LifeSize Gatekeeper. The maximum number of registrations allowed is shown on your license. The value shown on your license is the default setting.

License limit

Displays the maximum number of registrations that your license allows.

Note You may reduce the maximum number of calls or the maximum number of registrations while the LifeSize Gatekeeper is running. However, if currently there are more active calls than the new maximum, they will remain connected/registered until their completion.

BANDWIDTH (KBPS)

Check bandwidth rules

Check to enable the LifeSize Gatekeeper to compute and display used bandwidth in the **Inter-subzone Bandwidth Rules** and **Inter-zone Bandwidth Rules** dialog boxes in the Bandwidth Policy section of the **Bandwidth Policy** tab.

Reject call when bandwidth is insufficient

When checked, the LifeSize Gatekeeper rejects incoming calls when there is not enough bandwidth available for a specific call. When unchecked, the LifeSize Gatekeeper attempts to connect all calls regardless of bandwidth requirements, and sends a *BW capacity error* trap message. Available only when the **Check bandwidth rules** option is checked.

When bandwidth reaches limit

- **Ignore**—Select to instruct the LifeSize Gatekeeper to check all inter-zone and inter-subzone bandwidth rules and to calculate current bandwidth usage, but to ignore all bandwidth limitations.
- **Reduce**—Select to instruct the LifeSize Gatekeeper to reduce the bandwidth rate of a call to the allowed bandwidth rate when the requested bandwidth rate exceeds the allowed rate, and the allowed rate is equal to or greater than the rate configured in the **Minimum allowed *n* Kbps** field.

Note The LifeSize Gatekeeper rejects a call when the allowed bandwidth for a call is less than the rate configured in the **Minimum allowed *n* Kbps** field. In all other cases, the LifeSize Gatekeeper reduces the bandwidth to the allowed rate.

- **Minimum allowed *n* Kbps**—Indicates the reduced lower bandwidth rate of a call. When the **Reduce** option is selected and there is not enough available bandwidth for a call, the LifeSize Gatekeeper reduces the bandwidth rate of that call to the allowed rate provided that the allowed rate is equal to or greater than the rate configured in the **Minimum allowed *n* Kbps** field. The default value is 0.
- **Reject**—When checked, the LifeSize Gatekeeper rejects an incoming call when there is not enough bandwidth available for that call. When unchecked, the LifeSize Gatekeeper behaves according to which of the **Ignore** or **Reduce** options is selected.

DIAL PLAN

The **Dial Plan** section of the **Settings** tab enables you to configure the LifeSize Gatekeeper Dial Plan policy. You select with which version of the LifeSize Gatekeeper Dial Plan you want the LifeSize Gatekeeper to work in the **Basics** section of the **Settings** tab. Version 1 of the Dial Plan disables the **Dial Plan** section. For more Dial Plan information, see the LifeSize Gatekeeper Dial Plan version 2 appendix.

Note When the **Use Central Database** option is checked in the **Central Database** section of the **Settings** tab and **Version 2** is selected in the **Dial Plan version** field in the **Basics** section of the **Settings** tab, information displayed in the **Dial Plan** section is read-only.

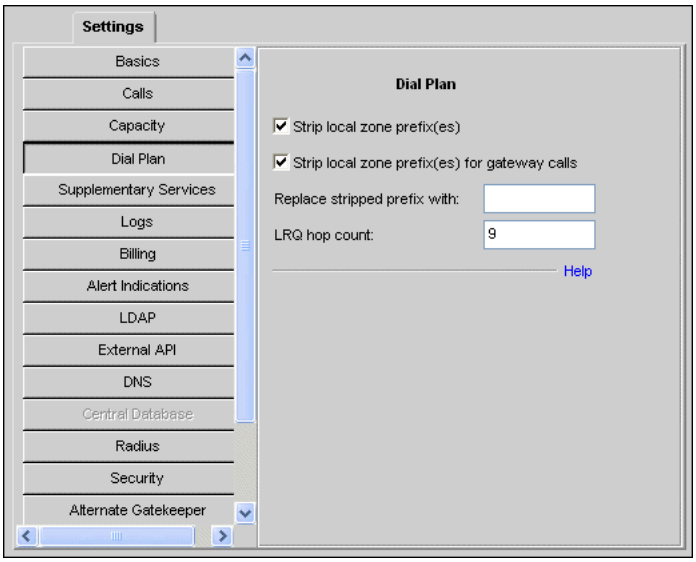

Figure 5-4 *Settings Tab: Dial Plan*

WHAT YOU CAN CONFIGURE

The following options are available for configuring the Dial Plan:

Note These options are available only in version 2 of the Dial Plan.

Strip local zone prefix(es)

When checked, enables the LifeSize Gatekeeper to strip its own zone prefixes in non-gateway calls (internal IP network calls).

For example, check this option if you want an endpoint to register without a zone prefix.

Strip local zone prefix(es) for gateway calls

When checked, enables the LifeSize Gatekeeper to strip its own zone prefixes in gateway calls (IP-to-ISDN network calls).

This option is for cases in which a call is dialed to a gateway and you want the LifeSize Gatekeeper to remove the local zone prefix from the number.

For example, you have a service 90, an ISDN number 03-7679408 (local zone prefix is 03), and someone on your network dials 90 03 7679408. When the **Strip local zone prefix(es) for gateway calls** option is checked, the gateway receives the number 90 7679408. If the option is unchecked, the gateway receives 90 03 7679408.

Note The **Strip local zone prefix(es)** and **Strip local zone prefix(es) for gateway calls** options are independent of each other.

Replace stripped prefix with

Enables you to replace a stripped zone prefix in gateway calls and/or non-gateway calls according to the selected stripping option(s). Enter the string with which you want the LifeSize Gatekeeper to replace zone prefixes. To replace a zone prefix with an empty string, check the appropriate stripping option(s) and leave the **Replace stripped prefix with** field empty.

LRQ hop count

Enter a whole number from 1 to 98 to set the maximum number of gatekeepers that an LRQ message can pass. The LRQ hop count prevents deadlocking when an LRQ loop occurs involving LifeSize Gatekeeper applications and non-LifeSize gatekeepers. At each gatekeeper in the loop, the LRQ hop count is reduced by 1 when that gatekeeper receives an LRQ. When a gatekeeper receives an LRQ and the LRQ hop count is 1, that gatekeeper reduces the LRQ hop count to 0 and sends an LRJ message. The default setting is 9.

Supplementary Services

The **Supplementary Services** section of the **Settings** tab enables you to specify H.450.2 and H.450.3 Supplementary Services. For more information, see H.450 Forwarding and Transfer on page 5.

Note Forwarding works with H.323 version 4-compliant endpoints only.

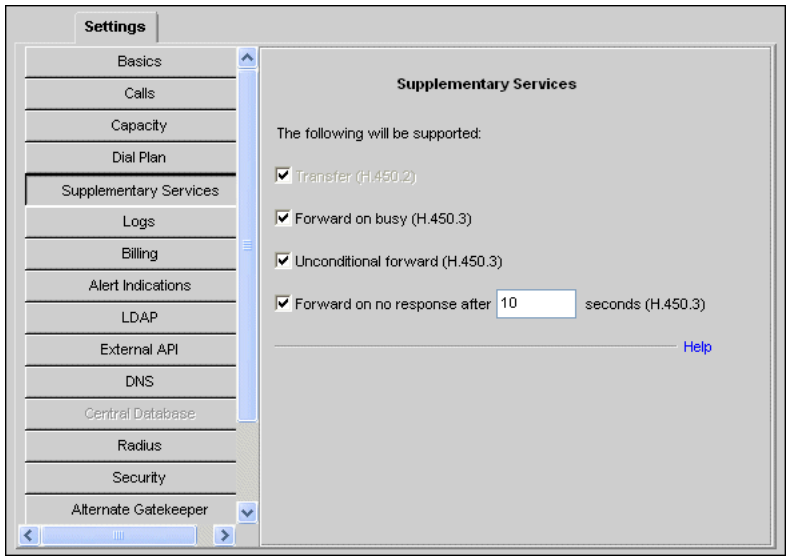

Figure 5-5 *Settings Tab: Supplementary Services*

WHAT YOU CAN CONFIGURE

The following options are available for configuring H.450 Supplementary Services:

Transfer (H.450.2)

Select this option to enable endpoint A to transform an existing call (from endpoint A to endpoint B) into a new call between endpoint B and an endpoint C, selected by endpoint A.

Note The **Transfer** option is always enabled; you cannot disable this checkbox. Endpoints must also support the H.450.2 Transfer Supplementary Service.

Forward on busy (H.450.3)

Select this option to enable an endpoint to have all its calls redirected to another endpoint when it is busy. The activating endpoint informs the LifeSize Gatekeeper to forward calls only when the activating endpoint is busy.

Unconditional forward (H.450.3)

Select this option to enable an endpoint to have all its calls redirected to another endpoint. The activating endpoint informs the LifeSize Gatekeeper to forward all calls without applying any conditions regarding the state of the diverted-from endpoint.

Forward on no response after *n* seconds (H.450.3)

Select this option to enable an endpoint to have its calls redirected to another endpoint when there is no response. Enter the time interval in seconds after which the calls are redirected if there is no response. The activating endpoint informs the LifeSize Gatekeeper to forward calls when there is no response from the forwarded-from endpoint within this time interval.

Note The H.450 Supplementary Service settings that you configure here also appear in the **Forwarding** section of the **Forward & Fallback** tab. For information on viewing Call Forwarding information, see the Forward & Fallback Tab chapter.

LOGS

The **Logs** section of the **Settings** tab enables you to define logging options for the LifeSize Gatekeeper and the H.245 Proxy.

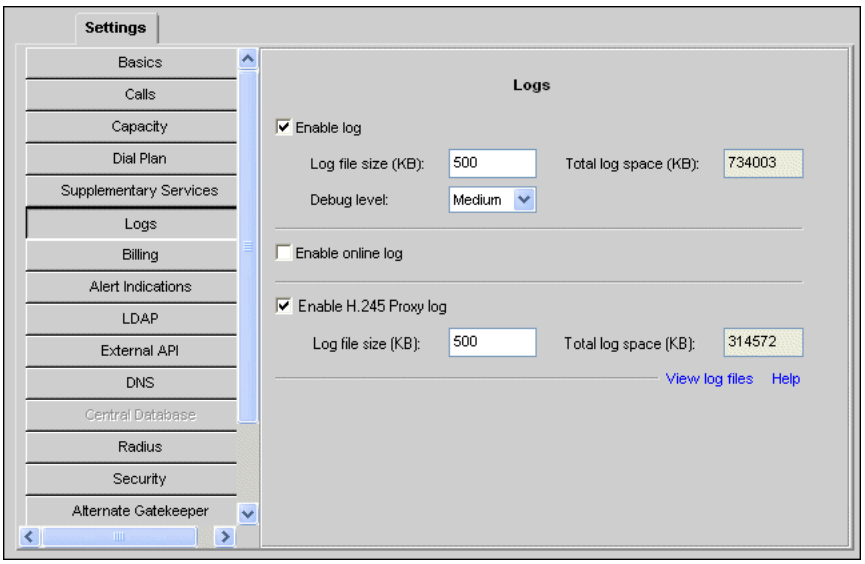

Figure 5-6 *Settings Tab: Logs*

ABOUT THE LOG

The LifeSize Gatekeeper saves the log data to a default file named *GK.log* located under the *Program Files* directory at:

Program Files\LifeSize\LifeSize Gatekeeper\Log\GK

When this file fills up, the LifeSize Gatekeeper automatically generates a new file called *GK0* followed by the date and the time (for example, *GK0_24/12/00_09:52*). When this file is full, the LifeSize Gatekeeper generates file *GK1* (followed by the date and time of this file generation), and so on. You can view these files in two ways:

- By clicking on the *Log* default directory icon which is located among the LifeSize Gatekeeper configuration files.
- By clicking on the **View log files** option at the bottom of the screen to open an FTP connection to the log files.

The log file numbering system is cyclical, starting from zero up to 10845. This limit is calculated by dividing 1GB by the size configured in the **Log file size (KB)** parameter. The default setting for the **Log file size (KB)** parameter is 100KB, giving a cyclic limit of 10845 (1,073,741,824 bytes divided by 1024 x 100).

When a log file reaches its size limit, the LifeSize Gatekeeper generates further log files of the size configured in the **Log file size (KB)** field. When the LifeSize Gatekeeper reaches the limit configured in the **Total log space (KB)** field, the log file writing mechanism returns to the first log file generated and begins to overwrite that file row by row.

Each time LifeSize Gatekeeper logging is enabled, the LifeSize Gatekeeper searches for the last file of the current log, according to the sequentially numbered file name. If this file has available space, the LifeSize Gatekeeper reopens the file for writing and records the reopening date and time at which the logging restarts. If this file is full, the LifeSize Gatekeeper generates a new log file and names this file with the next number in the sequence.

Note When restarting the computer, the LifeSize Gatekeeper clears the *Log* directory and starts the log numbering at 0. To save a log file, rename it prior to activating the LifeSize Gatekeeper.

LOG FILE FORMAT

The LifeSize Gatekeeper log files have the following format:

GKxx_dd-mm-yyyy-hh-mm-ss.log

where:

- “xx” is the cyclical file number starting from 0.
- “dd” is the day of the date when the file was closed.
- “mm” is the month of the date when the file was closed.
- “yyyy” is the year of the date when the file was closed.
- “hh” is the hour of the time when the file was closed.
- “mm” is the minutes of the time when the file was closed.
- “ss” is the seconds of the time when the file was closed.

The H.245 Proxy has the same logging system as the LifeSize Gatekeeper, with the following format:

MCxx_dd-mm-yyyy-hh-mm-ss.log

The numbering of the H.245 Proxy log files is independent of the LifeSize Gatekeeper log numbering. For more information about the H.245 Proxy, see About the H.245 Proxy on page 51.

Note H.245 Proxy logging is functional only when you enable the H.245 Proxy by setting the **Routing mode** option to **Call Setup (Q.931) and Call Control (H.245)** in the **Calls** section of the **Settings** tab.

What You Can Configure

The following options are available for configuring the log:

Enable log

Select this option to enable LifeSize Gatekeeper logging.

Log file size (KB)

Enter the maximum LifeSize Gatekeeper size limit for a single log file.

Total log space (KB)

Displays the maximum permissible size of all the LifeSize Gatekeeper log files combined.

Debug level

Select the required debug level—Minimal, Medium, High or Maximal. The debug details include reports of registrations and call transactions. The default setting is Medium.

Enable online log

When checked, opens an online window that displays all LifeSize Gatekeeper logging information. The window is located on the same computer as the LifeSize Gatekeeper and contains 1000 lines. Unchecked by default.

Enable H.245 P)roxy log

Select this option to enable H.245 Proxy logging.

Log file size (KB)

Displays the maximum size for a single H.245 Proxy log file.

Total log space (KB)

Displays the maximum permissible size of all the H.245 Proxy log files combined.

View log files

Opens an FTP connection for viewing the LifeSize Gatekeeper log files.

BILLING

The **Billing** section of the **Settings** tab enables you to define Call Detail Record (CDR) output for the LifeSize Gatekeeper. CDR output is created and sent on every call termination.

The LifeSize Gatekeeper either saves CDR data in a text file with a *.txt* extension, or sends CDR data to a specific billing server at an IP address, or both. The text file is saved in a default directory named CDR. The *CDR* directory is located in the LifeSize Gatekeeper directory. The file name is given a *cdr* prefix with the index number of the file you save, such as *cdr1.txt* and *cdr2.txt*. You can change the file name prefix and the file name extension of the text file. For more information on CDR, see the LifeSize Gatekeeper CDR Structure appendix.

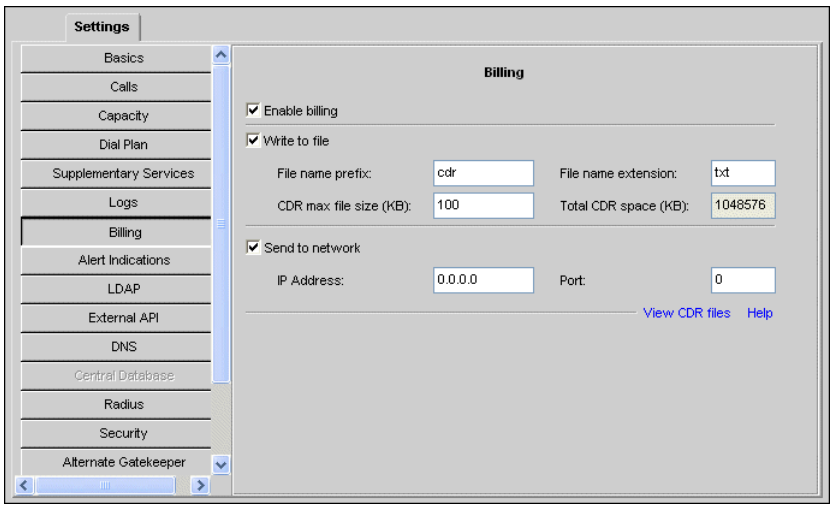

Figure 5-7 *Settings Tab: Billing*

WHAT YOU CAN CONFIGURE

The following options are available for configuring the billing information:

Enable billing

Select this option to enable the recording of billing data.

Note To enable CDR billing the LifeSize Gatekeeper must be configured to operate in the **Call Setup (Q.931)** or **Call Setup (Q.931) and Call Control (H.245)** routing modes. For more information about routing modes, see Calls on page 50.

Write to file

Select this option to enable billing data logging in a file.

File name prefix

Enter the prefix of the billing log file.

File name extension

Enter the extension of the billing log file.

CDR max file size (KB)

Displays the maximum size for a single CDR log file. When a new CDR is generated, the LifeSize Gatekeeper checks whether the new CDR will cause the log file to exceed the size configured in the **CDR max file size (KB)** field. If so, the LifeSize Gatekeeper opens a new log file and the maximum log file size is not exceeded.

Total CDR space (KB)

Displays the maximum permissible size for all the CDR log files combined.

Send to network

Select this option to enable data transmission to a billing server. Transmission is via the TPKT protocol over TCP/IP. In cases where the billing server stops working, the buffer contained within the TPKT protocol saves information transmitted from the CDR. On reconnection, this information safely reaches the billing server. On reconnection, the billing server itself is immediately available to receive CDR transmissions without the need for reconfiguration.

IP Address

Enter the IP address of the billing server.

Port

Enter the port number of the billing server.

View CDR files

Opens an FTP connection for viewing the LifeSize Gatekeeper CDR files.

ALERT INDICATIONS

The **Alert Indications** section of the **Settings** tab enables you to select which events cause the LifeSize Gatekeeper to send SNMP traps. You can define the SNMP servers to which the LifeSize Gatekeeper sends SNMP traps.

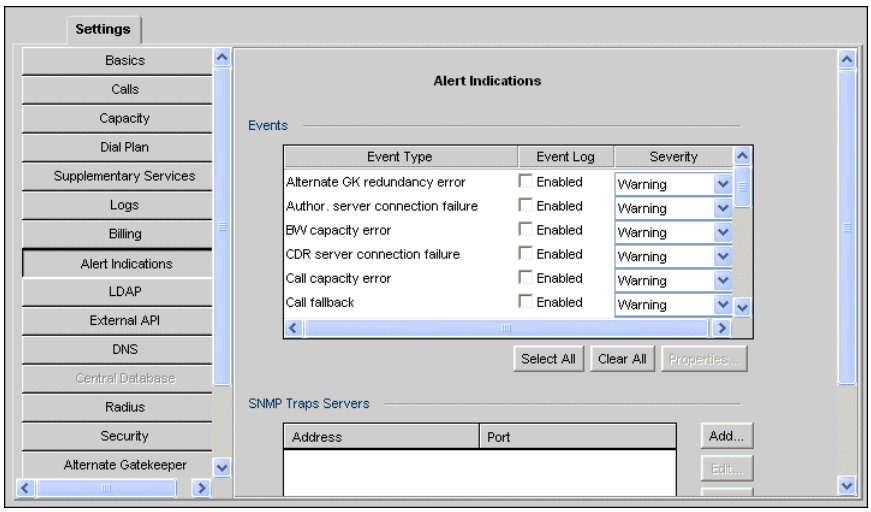

Figure 5-8 *Settings Tab: Alert Indications*

WHAT YOU CAN CONFIGURE

The following options are available for configuring alert indications:

EVENTS

Enable the events you want to monitor in the **Event Log** tab and designate a severity level for each event from the drop-down list.

Select All

Click to select all events simultaneously.

Clear All

Click to deselect all events currently selected.

Properties

You can configure capacity thresholds for certain event types, and the interval at which the LifeSize Gatekeeper checks communication with all Child Gatekeepers. Table 5-1 lists the configurable event types. For all other event types, this option is unavailable.

Table 5-1 *Event Type Properties Configuration*

Event Type	Configurable Property
BW capacity error	High and low capacity thresholds
Call capacity error	
Registration capacity error	
GK child is not alive	The interval at which the LifeSize Gatekeeper checks communication with all Child Gatekeepers

To configure capacity thresholds

1 Select **BW capacity error**, **Call capacity error** or **Registration capacity error** in the **Event Type** list, and click the **Properties** button. The **Event Properties** dialog box displays.

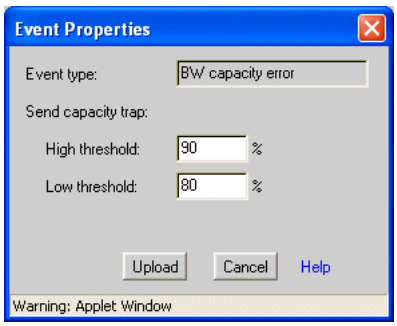

Figure 5-9 *Event Properties Dialog Box—BW Capacity Error*

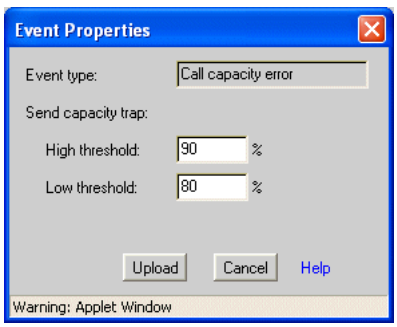

Figure 5-10 *Event Properties Dialog Box—Call Capacity Error*

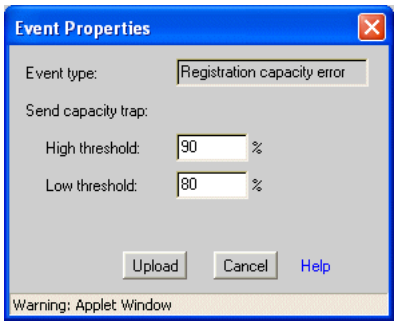

Figure 5-11 *Event Properties Dialog Box—Registration Capacity Error*

2 Set the required high and low capacity thresholds, and click **Upload**.

To set a Child Gatekeeper accessibility check interval

1 Select **GK child is not alive** in the **Event Type** list, and click the **Properties** button.

The **Event Properties** dialog box displays.

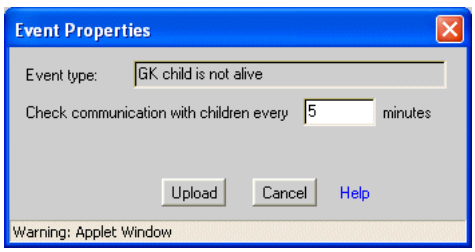

Figure 5-12 *Event Properties Dialog Box—GK Child is Not Alive*

2 Set the required interval at which the LifeSize Gatekeeper checks communication with all Child Gatekeepers, and click **Upload**.

SNMP Traps Servers

Displays the IP address and port number of configured SNMP traps servers. Click the **Add** and **Edit** buttons to display the **SNMP Trap Server Properties** dialog box for adding SNMP traps servers and modifying settings. For more information, see Adding and Modifying SNMP Traps Servers on page 71.

Adding and Modifying SNMP Traps Servers

The **SNMP Traps Server Properties** dialog box enables you to define the IP address, port and enabled traps for each SNMP traps server.

Type the traps server IP address, port number and use the **Add** and **Remove** buttons to select the traps you wish to monitor on the SNMP traps server.

The default port for SNMP traps servers is 162.

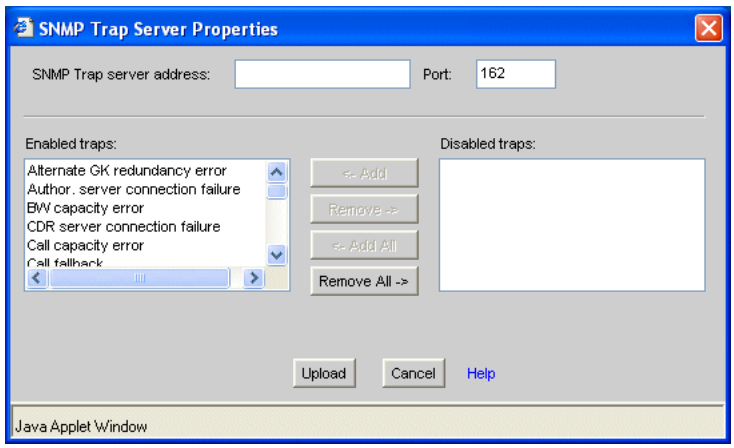

Figure 5-13 *SNMP Traps Servers Properties Dialog Box*

LDAP

The **LDAP** section of the **Settings** tab enables the LifeSize Gatekeeper to access LDAP directory services, including authentication, authorization, endpoint location, updating of endpoint information and retrieving Neighbor Gatekeeper lists.

Note The available configuration options vary depending on which option you select in the Schema type field. For more information, see Options available when the Gatekeeper schema is selected on page 76 and Options available when the H.350 schema is selected on page 79.

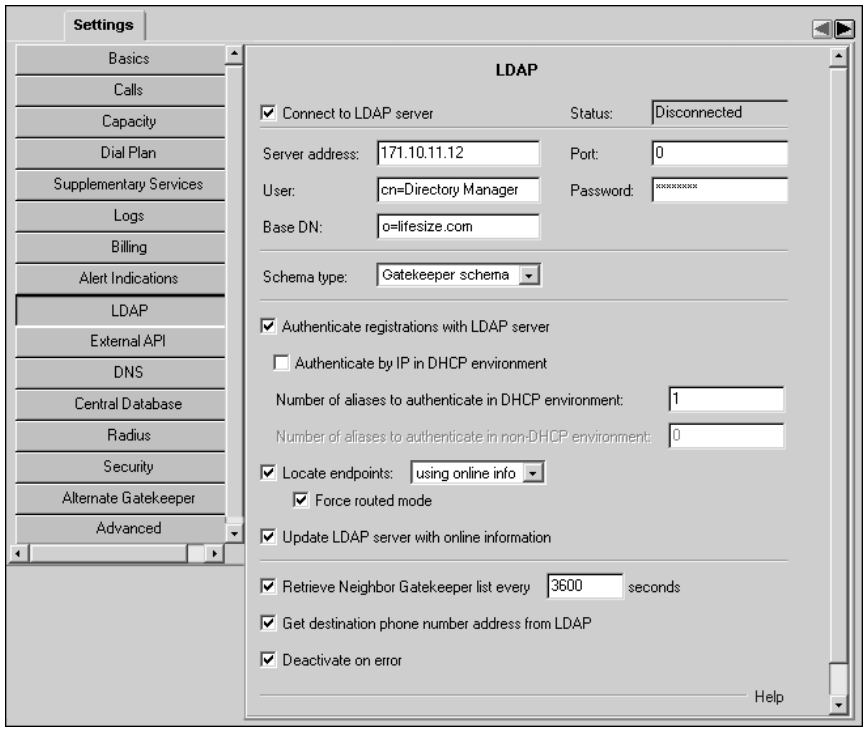

Figure 5-14 *Settings Tab: LDAP—Gatekeeper Schema*

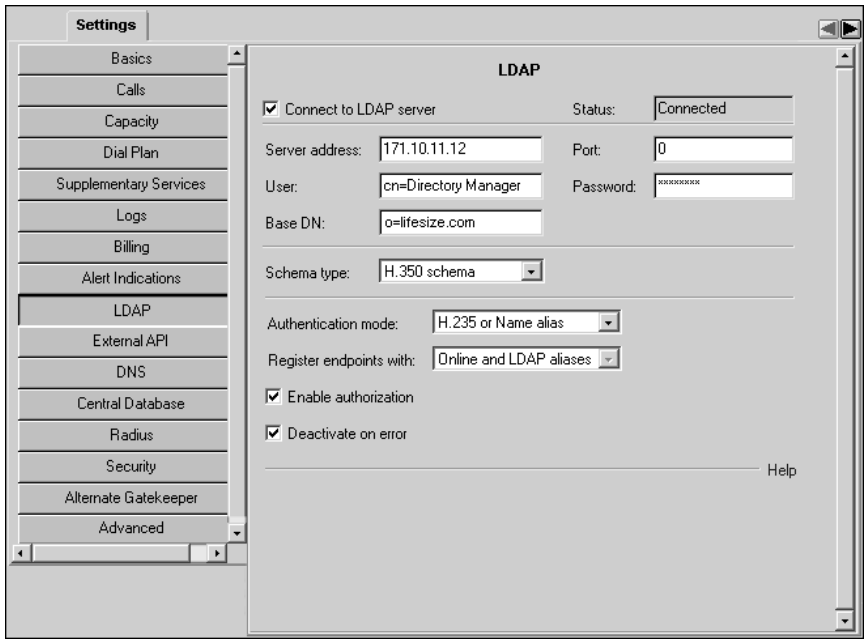

Figure 5-15 *Settings Tab: LDAP—H.350 Schema*

About LDAP

The Lightweight Directory Access Protocol (LDAP) is a protocol for accessing online directory services. LDAP is both an information model and a protocol for querying and manipulating the model. LDAP runs directly over TCP/IP and can be used to access a standalone LDAP directory service or to access a directory service that is back-ended by X.500—an overall model for Directory Services on the Open Systems Interconnection (OSI) model of network communications.

You need to configure LDAP to work with the LifeSize Gatekeeper. For more information, see the Configuring the LDAP Server chapter.

LDAP does not support a hierarchical LifeSize Gatekeeper structure. When using Dial Plan version 2 and the **Hierarchy** tab, you cannot use LDAP to locate endpoints or to retrieve Neighbor Gatekeepers. However, you can use LDAP for authenticating endpoints at registration when using Dial Plan version 2.

LifeSize Gatekeeper-LDAP Synchronization

The LifeSize Gatekeeper supports full synchronization with the LDAP server in cases of communication failure. On reconnection, the LifeSize Gatekeeper and the LDAP server are automatically synchronized.

The LDAP synchronization mechanism uses the *LDAP online information update failure* SNMP trap.

What You Can Configure

The following options are available for configuring LDAP information.

Connect to LDAP server

Select to activate all LDAP configuration fields.

Note When the **Connect to LDAP server** option is checked, information retrieved from the Central Database about Neighbor Gatekeepers is read-only. For more information about Neighbor Gatekeepers, see the Neighbors Tab chapter and the Hierarchy Tab chapter.

Status

Indicates the status of the LifeSize Gatekeeper connection to the LDAP server.

Note When working with an Alternate Gatekeeper, the connection status of the Slave LifeSize Gatekeeper is always shown as “Trying to connect” in the **Status** field.

Server address

Type the address of the LDAP server.

Port

Type the port number of the connection to the LDAP server, or use the default value **389**.

User

Type the name of the user with permission to access the LDAP server.

Password

Type the password of the user with permission to access the LDAP server.

Base DN

Type the name of the default tree in the LDAP server. If no prefix is defined, the LifeSize Gatekeeper automatically adds the prefix *o*= to the Base DN. For example, if you type *lifesize.com*, the LifeSize Gatekeeper modifies the Base DN string to *o*=*lifesize.com*.

Note You must not leave the **Base DN** field empty.

For more information, see the Configuring the LDAP Server chapter.

Schema type

Select the required schema from the drop-down list.

- **Gatekeeper schema**— A proprietary LifeSize schema enabling you to
  - Locate and update endpoints, and to retrieve a list of Neighbor Gatekeepers from the LDAP server.
  - Perform authentication according to endpoint alias and/or IP address.
- **H.350 schema**—The ITU-T H.350 standard schema for endpoints which support H.235 Annex D security, enabling you to
  - Perform authentication according to the H.235 sender identifier and password.

    Authentication of non-H.235 endpoints is performed according to the H.323 name alias and IP address.
  - Perform call authorization.

Note The available configuration options vary depending on which option you select in the **Schema type** field.

Options available when the Gatekeeper schema is selected

Authenticate registrations with LDAP server

Select to verify with the LDAP server if endpoints can register with a certain LifeSize Gatekeeper. For authentication to work, endpoints must be defined in the LDAP Static Information Tree. For more information, see To add a new entry to the Static Information Tree on page 254.

Note The LDAP server stores information on which endpoints can register with which LifeSize Gatekeeper. When an endpoint wishes to register with the LifeSize Gatekeeper, the LifeSize Gatekeeper checks against the LDAP server to see if the endpoint has access to it. This operation occurs at the Registration Request stage.

Authenticate by IP in DHCP environment

Check to instruct the LifeSize Gatekeeper to use endpoint IP addresses for authentication (in addition to aliases) when the LifeSize Gatekeeper operates in a DHCP environment.

Note The **Authenticate by IP in DHCP environment** option is enabled only when the **Authenticate registrations with LDAP server** option is checked, and when the DHCP environment in the zone option is checked in the Basics section of the **Settings** tab.

Number of aliases to authenticate in DHCP environment

Type the maximum number of alias matches that must be successfully made for an endpoint to be able to register to the LifeSize Gatekeeper in DHCP operation mode. For example, if you set this field to 4 and an endpoint is predefined in the LDAP server with 3 aliases, the endpoint must match at least 3 aliases. The default setting and the minimum allowed setting is 1.

The LifeSize Gatekeeper attempts to match an endpoint alias with the entries in the LDAP database. For more information about DHCP, see DHCP environment in the zone on page 48. For more information about configuring this option, see the Predefined Endpoint Authentication by Alias appendix.

Note The **Number of aliases to authenticate in DHCP environment** option is enabled only when the **Authenticate registrations with LDAP server** option is checked, and when the DHCP environment in the zone option is checked in the Basics section of the **Settings** tab.

Number of aliases to authenticate in non-DHCP environment

Type the maximum number of alias matches that must be successfully made for an endpoint to be able to register to the LifeSize Gatekeeper in non-DHCP operation mode (in addition to authentication according to IP address). For example, if you set this field to 4 and an endpoint is predefined in the LDAP server with 3 aliases, the endpoint must match at least 3 aliases. The default setting and the minimum allowed setting is 0.

Note When this field is set to 0, endpoint authentication is performed according to IP address only.

The LifeSize Gatekeeper attempts to match an endpoint alias with the entries in the LDAP database. For more information about DHCP, see DHCP environment in the zone on page 48. For more information about configuring this option, see the Predefined Endpoint Authentication by Alias appendix.

Note The **Number of aliases to authenticate in non-DHCP environment** option is enabled only when the **Authenticate registrations with LDAP server** option is checked, and when the DHCP environment in the zone option is unchecked in the Basics section of the **Settings** tab.

Locate endpoints

When checked, instructs the LifeSize Gatekeeper to resolve unrecognized aliases by sending an LDAP query to the LDAP server.

Note For the **Locate endpoints** feature to work, you must also check the **Retrieve Neighbor Gatekeeper list every *n* seconds** field below.

For more information about the LRQ policy of the LifeSize Gatekeeper, see Resolution of Aliases on page 9.

- Choose **using online info** to locate the address of an endpoint using dynamically registered information.

  The **Update LDAP server with online information** option must be selected.

- Choose **using static info** to locate the address of an endpoint using manually configured information. This option replaces the need to send a multicast LRQ to Neighbor Gatekeepers when an address is not found in the LifeSize Gatekeeper database.

  Endpoints must be registered in the LDAP Static Information Tree. For more information, see To add a new entry to the Static Information Tree on page 254.

Force routed mode

Select to force the LifeSize Gatekeeper to send a call to the destination endpoint gatekeeper, even if the destination gatekeeper is defined to operate in Direct Mode.

Update LDAP server with online information

Select to automatically update the LDAP server with dynamic endpoint information, such as if an endpoint registers or unregisters with the LifeSize Gatekeeper or changes an alias. Define each LifeSize Gatekeeper using this feature in the LDAP Online Information Tree. For more information, see To add a new entry to the Online Information Tree on page 256.

Retrieve Neighbor Gatekeeper list every *n* seconds

Check to retrieve updated information about Neighbor Gatekeepers from the Gatekeeper List Tree in the LDAP server. Set the time interval for retrieving the information. For information on Neighbor Gatekeepers, see the Neighbors Tab chapter.

Get destination phone number address from LDAP

Check to retrieve the destination address from the LDAP database. When an endpoint calls a destination alias which is not an E.164 alias, the LifeSize Gatekeeper retrieves the destination endpoint E.164 alias from the LDAP server.

Deactivate on error

Check to disable all LDAP-related parameters in the LifeSize Gatekeeper web interface when the connection to the LDAP server is lost. This feature enables you to continue working with the LifeSize Gatekeeper in cases of LDAP server error, such as network problems, invalid LDAP server password, invalid LDAP server address, and so on.

Warning When checked, endpoints can still register to the LifeSize Gatekeeper but the LifeSize Gatekeeper will not perform authentication or authorization.

OPTIONS AVAILABLE WHEN THE H.350 SCHEMA IS SELECTED

Authentication mode

Select the required endpoint authentication mode from the drop-down list.

- **None**—The LifeSize Gatekeeper performs no endpoint authentication.
- **H.235 only** (available only when the **Enable security (H.235)** option is checked in the Security section)—The LifeSize Gatekeeper authenticates endpoints using user name and password only, according to H.235 Annex D.
- **H.235 or Name alias** (available only when the **Enable security (H.235)** option is checked in the Security section)—The LifeSize Gatekeeper authenticates endpoints according to either
  - User name and password only

  or

- Name alias only

This option allows endpoints which do not support H.235 Annex D to register.

Note For more information about H.235 security, see Security on page 93.

Register endpoints with

When an endpoint registers with the LifeSize Gatekeeper, the LifeSize Gatekeeper stores the endpoint aliases retrieved from the LDAP server and from the endpoint RRQ message. Select the required alias type for endpoint registration from the drop-down list. Set to **Online aliases** when the **Authentication mode** option is set to **None**.

- **LDAP aliases**—The LifeSize Gatekeeper uses only the endpoint alias retrieved from the LDAP server.
- **Online aliases**—The LifeSize Gatekeeper uses only the endpoint aliases provided in the RRQ message.
- **Online and LDAP aliases**—The LifeSize Gatekeeper uses both the endpoint aliases provided in the RRQ message and the endpoint alias retrieved from the LDAP server.

Enable authorization

Check to enable authorization. When checked, the LifeSize Gatekeeper retrieves the service level defined for the endpoint in the LDAP server.

Note You must define a group using the same name as you used for defining the endpoint service level in the LDAP server. You must also check the **Add members according to LDAP information** option in the **Add Group** dialog box. For more information, see Adding or Modifying a Group on page 143.

Get Caller ID presentation policy

When checked, the LifeSize Gatekeeper verifies in the LDAP server whether or not the presentation of the calling endpoint ID is allowed to the receiving endpoint. If yes, the ID of the calling endpoint is visible to the receiving endpoint when the LifeSize Gatekeeper connects the call. If no, the ID of the calling endpoint is not presented to the receiving endpoint.

When unchecked, the LifeSize Gatekeeper attempts to connect the call without referring to the LDAP server for the ID presentation policy of the calling endpoint.

Checked by default.

Deactivate on error

Check to disable all LDAP-related parameters in the LifeSize Gatekeeper web interface when the connection to the LDAP server is lost. This feature enables you to continue working with the LifeSize Gatekeeper in cases of LDAP server error, such as network problems, invalid LDAP server password, invalid LDAP server address, and so on.

Warning When checked, endpoints can still register to the LifeSize Gatekeeper but the LifeSize Gatekeeper will not perform authentication or authorization.

EXTERNAL API

The **External API** section of the **Settings** tab enables you to allow external servers to connect to the LifeSize Gatekeeper and displays connected servers.

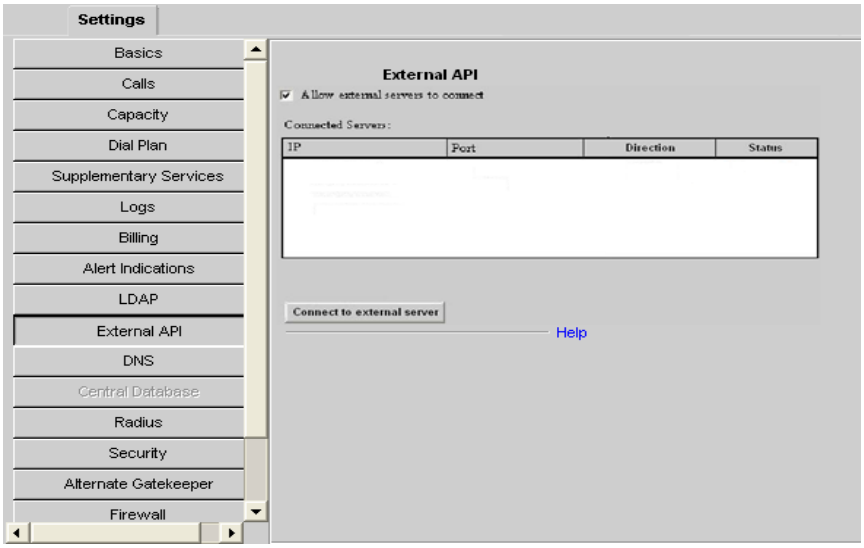

Figure 5-16 *Settings Tab: External API*

What You Can Configure

The following configuration options are available in the **External API** section:

Allow external servers to connect

Check to enable external authorization server applications to communicate with the LifeSize Gatekeeper.

Connect to external server

Available only when the LifeSize Gatekeeper is enabled to initiate connections with an external server. Click to configure external authorization servers with which the LifeSize Gatekeeper can initiate communication. For more information, see Connecting to an External Authorization Server.

What You See

The following information is displayed in the **External API** section:

Table 5-2 *External Servers Table*

Field	Description
IP	Displays the IP address of external authorization servers that are connected to the LifeSize Gatekeeper.
Port	Displays the destination port used by external authorization servers for communication with the LifeSize Gatekeeper.
Direction	Available only when the LifeSize Gatekeeper is enabled to initiate connections with an external server. Displays the direction of the connection with the external authorization server from the point of view of the LifeSize Gatekeeper.
Status	Available only when the LifeSize Gatekeeper is enabled to initiate connections with an external server. Displays the status of the connection between the LifeSize Gatekeeper and the external server.

Connecting to an External Authorization Server

The Connect to External Server button enables you to configure the LifeSize Gatekeeper to initiate a connection to an external authorization server application.

Enable Server

Check to enable the external server.

Server address

Type the IP address of the external server.

Port

Type the port number of the external server.

User

Type a user name for access to the external server.

Password

Type a password for access to the external server.

Upload

Click to upload your changes to the LifeSize Gatekeeper database.

DNS

The **DNS** (Domain Name Server) section of the **Settings** tab enables you to configure parameters to resolve e-mail and URL aliases using a DNS server when the LifeSize Gatekeeper cannot find a destination.

About DNS

When the LifeSize Gatekeeper cannot resolve a call within the LifeSize Gatekeeper zone, and the destination contains e-mail and/or URL aliases, the LifeSize Gatekeeper can contact a preconfigured DNS server and receive a list of gatekeepers relevant to the queried domain. The list is a prioritized list of gatekeeper IP addresses within the given domain. These IP addresses are resolved via DNS queries according to procedures recommended in H.225.0 version 2.

Upon receiving the full list of gatekeeper IP addresses, the LifeSize Gatekeeper issues LRQ messages to all the gatekeepers on the list in order to establish the location of the destination endpoint.

Automatic E-mail Address Generation

The LifeSize Gatekeeper can automatically generate an e-mail address from H.323 aliases according to the domain configured in the **Local Domain** field of the **DNS** section. For more information, see Automatic E-mail Address Generation on page 11.

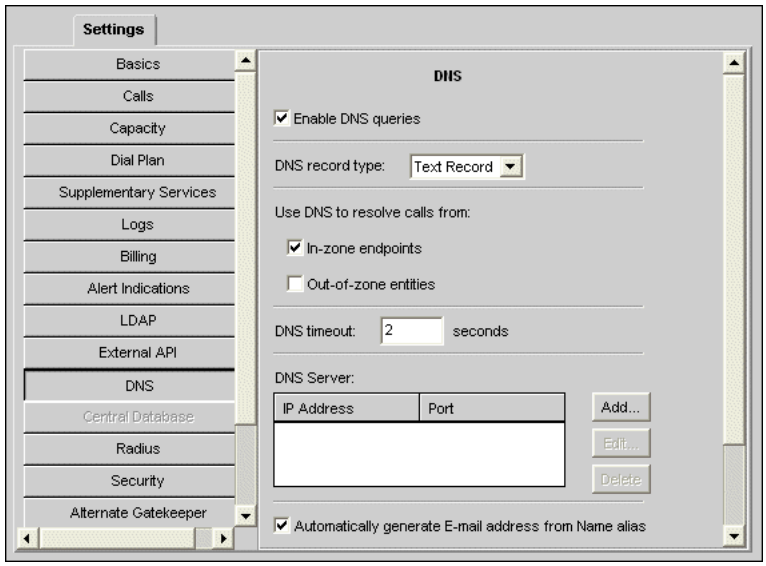

Figure 5-17 *Settings Tab: DNS*

WHAT YOU CAN CONFIGURE

The following options are available for configuring DNS settings:

Enable DNS queries

When checked, instructs the LifeSize Gatekeeper to resolve unrecognized aliases by sending a Location Request message (LRQ) to the DNS server. For more information about the LRQ policy of the LifeSize Gatekeeper, see Resolution of Aliases on page 9.

DNS record type

Select the required DNS record type from the drop-down list.

- **Text Record**

  Enables the LifeSize Gatekeeper to request that the DNS server returns non-standard TXT type records only.

- **A Record**

  Enables the LifeSize Gatekeeper to request that the DNS server returns Host (A) type records only.

Use DNS to resolve calls from

- **In-zone endpoints**

  When checked, enables the LifeSize Gatekeeper to resolve destination addresses for calls originating from in-zone endpoints.

- **Out-of-zone entities**

  When checked, enables the LifeSize Gatekeeper to resolve destination addresses for calls originating from out-of-zone entities.

DNS timeout

The connection timeout (in seconds) between the LifeSize Gatekeeper and the DNS server to which the LifeSize Gatekeeper sends a query.

DNS Server

Displays the DNS server to which the LifeSize Gatekeeper has access.

Add

Click to add a DNS server. Unavailable if a DNS server is already configured. For more information, see Adding or Modifying DNS Server Details on page 86.

Edit

Double click the DNS server, or select the DNS server and click **Edit** to modify DNS settings. For more information, see Adding or Modifying DNS Server Details on page 86.

Delete

Click to remove the DNS server.

Automatically generate E-mail address from Name alias

When checked, the LifeSize Gatekeeper automatically generates an e-mail address from H.323 aliases in incoming ARQ, RRQ and LRQ messages according to the domain configured in the **Local Domain** field. For more information, see Automatic E-mail Address Generation on page 11.

Local Domain

Type the local domain for e-mail address generation. When an incoming RRQ H.323 Name alias does not contain the "@" symbol, the LifeSize Gatekeeper generates an e-mail address using the value in the **Local Domain** field. For more information, see Automatic E-mail Address Generation on page 11.

Adding or Modifying DNS Server Details

To add a DNS server, click **Add** to display the **Add DNS Server** dialog box. To modify an existing DNS server, select the server in the **DNS** section of the **Settings** tab and click **Edit**, or double click the server to display the **Edit DNS Server** dialog box.

The following options are available in the **Add DNS Server** or **Edit DNS Server** dialog box:

IP Address

Enter or modify the IP address of the DNS server.

Port

Enter or modify the port number of the DNS server.

OK

Click the **OK** button to upload the DNS server information to the LifeSize Gatekeeper database.

CENTRAL DATABASE

The **Central Database** section of the **Settings** tab enables you to configure the LifeSize Gatekeeper connection to an SQL database.

The Central Database is distinct from the LifeSize Gatekeeper database referred to elsewhere in this manual.

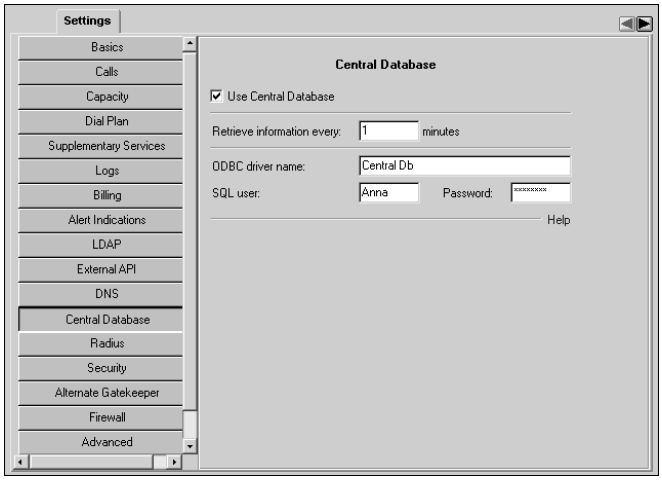

Figure 5-18 *Settings Tab: Central Database*

ABOUT THE CENTRAL DATABASE

The Central Database is an SQL database containing information about every gatekeeper on the network. Each new LifeSize Gatekeeper sends its IP address to the SQL server on joining the network. Each LifeSize Gatekeeper on the network calls the SQL server at a predefined interval to receive updated information about itself.

Information held in the Central Database includes the following:

- The name and IP address of the LifeSize Gatekeeper.
- The names and IP addresses of the parent, neighbors and children of the LifeSize Gatekeeper.
- Whether or not the LifeSize Gatekeeper strips prefixes on gateway calls.
- Whether or not the LifeSize Gatekeeper strips prefixes on non-gateway calls.
- The zone prefixes configured on the LifeSize Gatekeeper.

- The string with which the gatekeeper replaces specified zone prefixes.
- The global services configured on the LifeSize Gatekeeper.

Note When the **Use Central Database** option is checked and **Version 2** is selected in the **Dial Plan version** field in the **Basics** section of the **Settings** tab, the information displayed in the **Dial Plan** section of the **Settings** tab, in the **Global Services** section of the **Services** tab and in the **Hierarchy** tab is read-only.

Accessing the Central Database

Communication with the SQL database is based on the ODBC standard. The SQL server identifies each LifeSize Gatekeeper by a unique identifier. You define the LifeSize Gatekeeper identifier in the **Gatekeeper ID** field in the **Basics** section of the **Settings** tab. LifeSize Gatekeeper admission to the SQL server is authenticated at the ODBC level by a name and password which are common to every LifeSize Gatekeeper on the network.

What You Can Configure

The following options are available for configuring the Central Database:

Use Central Database

When checked, enables the LifeSize Gatekeeper to access the Central Database.

Retrieve information every *n* minutes

Enter the time interval at which you want the LifeSize Gatekeeper to download updated information about itself from the Central Database.

ODBC driver name

Enter the name of the ODBC driver you use to access the SQL server containing the Central Database.

SQL user

Enter the name of the SQL server user.

Password

Enter the password of the SQL server user.

RADIUS

The **Radius** section of the **Settings** tab enables you to check LifeSize Gatekeeper-registered endpoints against a RADIUS (Remote Access Dial-In User Service) server for authentication, authorization and accounting. RADIUS is the de facto standard for authentication, authorization and accounting.

The LifeSize Gatekeeper supports connections to RFC 2865-compliant and Shiva Access Manager (SAM) servers.

The LifeSize Gatekeeper RADIUS module ensures that where an endpoint has multiple aliases, all authenticated aliases are associated with that endpoint in the RADIUS server database.

The LifeSize Gatekeeper encapsulates all endpoint aliases in the same RADIUS request packet.

SPECIFYING YOUR AUTHENTICATION POLICY

You configure authentication policy preferences via the registry.

You specify authentication policy options using the **RADIUSAuthenticationPolicy** registry string under the registry key

---

Note Stop the LifeSize Gatekeeper before specifying the authentication policy option you require.

`HKLM\SOFTWARE\LifeSize\LifeSize Gatekeeper\Parameters\RADIUS`

The **RADIUSAuthenticationPolicy** value determines the authentication policy as follows (the value is of type **REG_DWORD**):

- 1 = “Any alias”—At least one endpoint alias should be authenticated.
- 2 = "At least 2"—At least two endpoint aliases should be authenticated.
- 3 = "At least 3"—At least three endpoint aliases should be authenticated.
- 4 = "At least 4"—At least four endpoint aliases should be authenticated.
- 5 = "All aliases"—All endpoint aliases should be authenticated.
- 6 = “H.323"—At least one name alias should be authenticated.
- 7 = "URL"—At least one URL alias should be authenticated.
- 8 = "E-Mail"—At least one e-mail alias should be authenticated.
- 9 = "E.164"—At least one phone alias should be authenticated.

- 10 = "Transport"—At least one transport address should be authenticated.
- 11 (default) = “All aliases (one packet)”—All endpoint aliases should be authenticated, and all endpoint aliases are encapsulated in the same RADIUS request packet.

Note The total length of all the aliases must not exceed 256 characters.

Customizing Alias Formats

The LifeSize Gatekeeper encapsulates all the aliases for a given endpoint in the *Username* attribute of the RADIUS request packet. The *Username* attribute has the format < TYPE>:< LENGTH>:<STRING> for each alias, where

- <TYPE> represents the alias type—one of:

  N = name

  P = phone

  E = e-mail

  U = URL

  T = transport
- <LENGTH> represents the alias string length
- <STRING> represents the ASCII representation of the alias

You customize alias formats using the **RADIUSOnePacket** set of registry strings under the registry key

`HKLM\SOFTWARE\LifeSize\LifeSize Gatekeeper\Parameters\RADIUS`

The **RADIUSOnePacket** value determines the alias format as follows (all values are of type **REG_SZ**):

- **RADIUSOnePacketFormat**—One alias format string. The default value is **%t:%l:%s:**, where

  %t is substituted by the alias type tag

  %l is substituted by the alias string length in characters

  %s is substituted by the alias string itself
- **RADIUSOnePacketName**—Name alias tag. The default value is N.
- **RADIUSOnePacketPhone**—Phone (E.164) alias tag. The default value is P.
- **RADIUSOnePacketEmail**—E-mail alias tag. The default value is E.
- **RADIUSOnePacketURL**—URL alias tag. The default value is U.

- **RADIUSOnePacketTransport**—Transport alias tag. The default value is T.

Note Stop the LifeSize Gatekeeper before specifying the alias format you require.

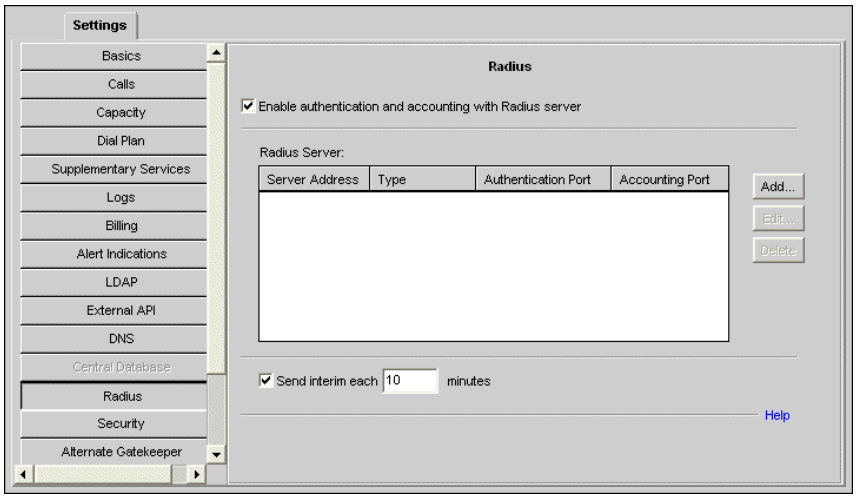

Figure 5-19 *Settings Tab: Radius*

WHAT YOU CAN CONFIGURE

The following configuration options are available in the **Radius** section:

Enable authentication and accounting with Radius server

Check to enable the LifeSize Gatekeeper to connect with a RADIUS server.

Radius Server

Displays details of the RADIUS server to which the LifeSize Gatekeeper is currently connected.

Add

Click to add a RADIUS server. Unavailable if the LifeSize Gatekeeper is currently connected to a RADIUS server. For more information, see Adding or Modifying RADIUS Server Details on page 92.

Edit

Double click the RADIUS server, or select the RADIUS server and click **Edit** to modify the specified server entry. For more information, see Adding or Modifying RADIUS Server Details on page 92.

Delete

Click to remove a RADIUS server entry.

Send interim each *n* minutes

Check to enable the LifeSize Gatekeeper to send interim billing reports to the RADIUS server. Set the interval at which the LifeSize Gatekeeper sends billing information to the RADIUS server to between 1 and 60 minutes.

Adding or Modifying RADIUS Server Details

To add a RADIUS server, click **Add** to display the **Add Radius Server** dialog box. To modify an existing RADIUS server, select the server in the **Radius** section of the **Settings** tab and click **Edit**, or double click the server to display the **Edit Radius Server** dialog box.

The following options are available in the **Add Radius Server** or **Edit Radius Server** dialog box:

Server address

Type the address of the RADIUS server.

Type

Select the required type from the drop-down list—**RFC Compliant** refers to RFC 2865; **Shiva** refers to the Shiva Access Manager (SAM) server.

Authentication port

Configure an authentication port for the RADIUS server. By default, RFC Compliant and Shiva servers communicate via port 1812.

Accounting port

Configure an accounting port for the RADIUS server. By default, RFC Compliant servers communicate via port 1813; Shiva servers communicate via port 1812.

Note The **Authentication port** and **Accounting port** fields refer to ports on the RADIUS server, and not on the LifeSize Gatekeeper.

Secret

Type a shared secret password or key. The shared secret between the LifeSize Gatekeeper and the RADIUS server forms the basis of the security process. Only the LifeSize Gatekeeper and the RADIUS server know the shared secret.

Whenever the LifeSize Gatekeeper sends a message to the RADIUS server, the LifeSize Gatekeeper encrypts the message using the password. The RADIUS server authenticates the message using the same password. If one of the parties does not have the correct password, the authentication fails and the transaction is rejected.

User name

Type a user name for the RADIUS server.

SECURITY

In the **Security** section of the **Settings** tab you can enable H.235 Annex D security to ensure the authentication of each endpoint and the integrity of messages.

ABOUT H.235 SECURITY

The basis of the security process is the shared secret between the endpoint and the LifeSize Gatekeeper. This shared secret can be either a password or a key. Only the endpoint and the LifeSize Gatekeeper know the shared secret.

Authentication and Integrity are achieved by encrypting part of the entire message using the shared secret. Whenever an endpoint sends a message to the LifeSize Gatekeeper, the endpoint encrypts the message using the password. The

LifeSize Gatekeeper authenticates the message using the same password. If one of the parties does not have the correct password, the authentication fails and the call is rejected.

Note LifeSize Gatekeeper H.235 security works with endpoints that support H.235 Annex D and certain TANDBERG proprietary algorithms.

WHAT YOU CAN CONFIGURE

The following options are available for configuring H.235 security:

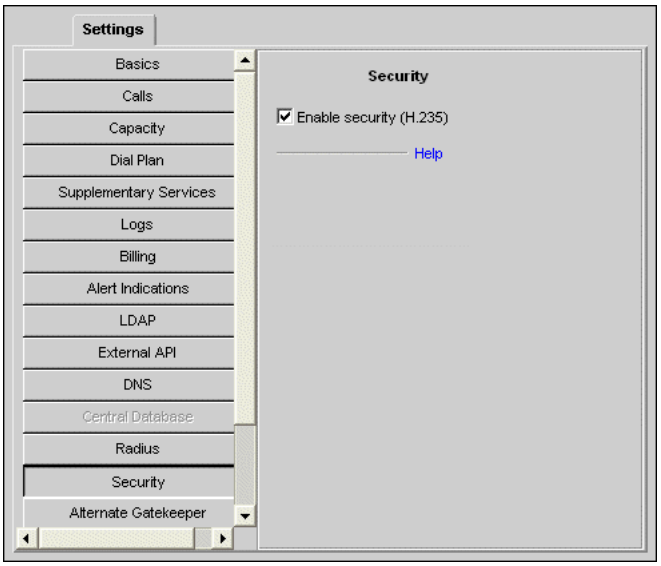

Figure 5-20 *Settings Tab: Security*

Enable security (H.235)

When checked, enables the LifeSize Gatekeeper to work with H.235 authentication and integrity security. H.235 version 2 authentication and integrity combines Authentication and Integrity based on H.235 Annex D.

Alternate Gatekeeper

The **Alternate Gatekeeper** section of the **Settings** tab enables you to configure a backup "Alternate" LifeSize Gatekeeper to provide high availability of gatekeeper services.

High availability makes LifeSize Gatekeeper failures transparent to the endpoints that are registered to the LifeSize Gatekeeper. A backup LifeSize Gatekeeper (the "Alternate Gatekeeper") runs in parallel to each online LifeSize Gatekeeper. The LifeSize Gatekeeper builds and saves a Registration Table. The Alternate Gatekeeper copies and uploads this Registration Table. If the LifeSize Gatekeeper goes offline, the Alternate Gatekeeper replaces the LifeSize Gatekeeper **within ten seconds**.

The Alternate Gatekeeper license is limited to 14 days. The 14-day period restarts every time the online and backup LifeSize Gatekeeper switch roles.

Note The Alternate Gatekeeper mechanism described here is proprietary to LifeSize and is distinct from the Alternate Gatekeeper mechanism of the H.323 standard.

About the Alternate Gatekeeper Feature

To use the Alternate Gatekeeper feature, you install and operate two identical LifeSize Gatekeeper instances. All Setup configuration information for the two LifeSize Gatekeeper instances must be identical. One LifeSize Gatekeeper assumes the role of the master gatekeeper (the *Primary* LifeSize Gatekeeper) and the other assumes the role of the slave gatekeeper (the *Secondary* LifeSize Gatekeeper). When the Primary LifeSize Gatekeeper goes offline, the Secondary LifeSize Gatekeeper becomes the master. These roles remain unchanged until the new master LifeSize Gatekeeper goes offline.

When the LifeSize Gatekeeper is set to work in Direct Mode with the **Force Direct Mode for service calls** option checked in the **Advanced** section of the **Settings** tab, the management of calls in progress when the Primary LifeSize Gatekeeper goes offline passes to the endpoints involved in the call. Calls made under any other mode are lost when the Primary LifeSize Gatekeeper goes offline.

Note When you enable the Alternate Gatekeeper feature by checking the **Use Alternate Gatekeeper** option and clicking the **Upload** button, the role of the LifeSize Gatekeeper in the Alternate Gatekeeper environment (**Master** or **Slave**) is shown after the Gatekeeper identifier indication on the right side of the toolbar. The role indication appears on *all* LifeSize Gatekeeper screens.

Windows IP Addressing

Every Microsoft Windows system includes a Native IP address. The Native IP address is the unique IP address that defines the location on the network of the system.

Each system IP address has a subnet mask. All system-level IP addresses must have the same subnet mask in both the Primary and the Secondary LifeSize Gatekeeper.

Alternate Gatekeeper IP Addressing

The **Alternate Gatekeeper** section of the **Settings** tab includes three IP address fields, a ping interval configuration field and a port configuration option:

- **Alternate Gatekeeper Native IP**

  The Native IP of the "other" LifeSize Gatekeeper. When you configure the Primary LifeSize Gatekeeper, enter the Native IP address of the Secondary LifeSize Gatekeeper. When you configure the Secondary LifeSize Gatekeeper, enter the Native IP address of the Primary LifeSize Gatekeeper.

- **Public Gatekeeper IP**

  The IP address that will be used as the publicly available IP address of the LifeSize Gatekeeper.

Note You must manually configure the Native IP address of the Primary and Secondary LifeSize Gatekeeper on your host operating system.

- **Probe IP**

  The IP address with which the slave LifeSize Gatekeeper communicates when checking the status of the slave LifeSize Gatekeeper connection to the network. The status of the slave connection to the network determines whether or not a problem is local to the slave. LifeSize recommends that you do the following:

  - Configure the Primary and the Secondary LifeSize Gatekeepers with the same Probe IP address.
  - Configure the IP address of the network default gateway as the Probe IP address. When there is no network default gateway, configure the IP address of a server on the network that is always online.

- **Ping Interval**

  The slave LifeSize Gatekeeper pings the master LifeSize Gatekeeper at preconfigured intervals to check the status of the slave LifeSize Gatekeeper connection to the network. When the slave LifeSize Gatekeeper does not receive a response from the master LifeSize Gatekeeper, the slave LifeSize Gatekeeper checks the status of its connection to the network by pinging the Probe IP address. A response from the Probe IP address indicates that the slave LifeSize Gatekeeper is connected to the network and that the master LifeSize Gatekeeper has gone offline. The lack of a response from the Probe IP address indicates that the slave LifeSize Gatekeeper is not properly connected to the network.

- **Inter-gatekeeper Communication Port**

  The TCP/IP port through which the Primary and the Secondary LifeSize Gatekeeper establish a reliable connection for communication with each other. The port number must be the same on both the Primary and the Secondary LifeSize Gatekeeper.

Sample Alternate Gatekeeper Configuration

The following example shows how to configure the fields in the **Alternate Gatekeeper** section of the **Settings** tab using the system-level addressing information.

In the example

- The two LifeSize Gatekeeper share a common Public IP address (172.20.77.100).
- The default gateway IP address (172.20.77.254) also serves as the Probe IP address.

Perform Alternate Gatekeeper configuration according to the following steps:

To configure the Alternate Gatekeeper feature

1. Perform LifeSize Gatekeeper 1 system-level configuration.
2. Perform LifeSize Gatekeeper 2 system-level configuration.
3. Configure the LifeSize Gatekeeper 1 **Alternate Gatekeeper** section of the **Settings** tab.
4. Configure the LifeSize Gatekeeper 2 **Alternate Gatekeeper** section of the **Settings** tab.
5. Restart LifeSize Gatekeeper 1 and LifeSize Gatekeeper 2.

Step 1—LifeSize Gatekeeper 1 System-level configuration

1. Native IP address (172.20.77.10)—unique.
2. Default gateway IP address (172.20.77.254)—common to LifeSize Gatekeeper 1 and LifeSize Gatekeeper 2.

Step 2—LifeSize Gatekeeper 2 System-level configuration

1. Native IP address (172.20.77.1)—unique.
2. Default gateway IP address (172.20.77.254)—common.

Step 3—LifeSize Gatekeeper 1 Alternate Gatekeeper configuration

1. **Alternate Gatekeeper Native IP** (172.20.77.1)—Native IP address of LifeSize Gatekeeper 2.
2. **Public Gatekeeper IP** (172.20.77.100)—common.
3. **Probe IP** (172.20.77.254)—common default gateway IP address.

Step 4—LifeSize Gatekeeper 2 Alternate Gatekeeper configuration

1. **Alternate Gatekeeper Native IP** (172.20.77.10)—Native IP address of LifeSize Gatekeeper 1.
2. **Public Gatekeeper IP** (172.20.77.100)—common.
3. **Probe IP** (172.20.77.254)—common default gateway IP address.

Step 5—Restart LifeSize Gatekeeper 1 and LifeSize Gatekeeper 2

Figure 5-21 on page 99 illustrates the Alternate Gatekeeper configuration described here.

Figure 5-21 Sample Alternate Gatekeeper Configuration

ALTERNATE GATEKEEPER PROCEDURE

This section describes how the Secondary LifeSize Gatekeeper replaces the Primary LifeSize Gatekeeper when the Primary LifeSize Gatekeeper goes offline when in the master LifeSize Gatekeeper role.

The Primary LifeSize Gatekeeper goes offline

1. The Secondary LifeSize Gatekeeper checks its connection to the Primary LifeSize Gatekeeper but does not receive a response.
2. The Secondary LifeSize Gatekeeper checks its connection to the network at the **Probe IP** address (172.20.77.254) and does receive a response.
3. The Secondary LifeSize Gatekeeper services the network by assuming the master LifeSize Gatekeeper role and by adding the Public Gatekeeper IP address (172.20.77.100) to its list of given IP addresses. The Secondary LifeSize Gatekeeper now has two live system-level IP addresses—Native and Public. Endpoints are registered to the Public Gatekeeper IP address.

The Primary LifeSize Gatekeeper comes back online

1. The Primary LifeSize Gatekeeper re-establishes a TCP/IP connection with the Secondary LifeSize Gatekeeper.
2. The Primary LifeSize Gatekeeper queries its status with the Secondary LifeSize Gatekeeper.
3. The Secondary LifeSize Gatekeeper notifies the Primary LifeSize Gatekeeper that the Secondary LifeSize Gatekeeper is the master.
4. The Primary LifeSize Gatekeeper assumes the slave role.
5. The Secondary LifeSize Gatekeeper transfers all current registrations to the Primary LifeSize Gatekeeper.
6. The Primary LifeSize Gatekeeper remains in the slave role until the Secondary LifeSize Gatekeeper goes offline.
7. The Primary LifeSize Gatekeeper detects if the Secondary LifeSize Gatekeeper has gone offline by checking its connection to the Secondary LifeSize Gatekeeper.
8. If the Primary LifeSize Gatekeeper does not receive a response, the Primary LifeSize Gatekeeper checks its connection to the network at the **Probe IP** address (172.20.77.254). If it does receive a response, the Primary LifeSize Gatekeeper services the network by assuming the master LifeSize Gatekeeper role, and the Alternate Gatekeeper mechanism runs as described at step 3 of the The Primary LifeSize Gatekeeper goes offline section.

Note The LifeSize Gatekeeper sends an SNMP trap each time the roles of the Primary and Secondary LifeSize Gatekeeper change.

Updating Static Information

Static information includes all configuration information and information on predefined endpoints. You must manually update the slave LifeSize Gatekeeper with any changes to the master LifeSize Gatekeeper static information. Save the new information to a file using the **Export** button on the toolbar of the LifeSize Gatekeeper Administrator configuration interface. Upload the new information file to the slave LifeSize Gatekeeper using the **Import** button on the toolbar of the LifeSize Gatekeeper Administrator configuration interface.

Updating Dynamic Information

Dynamic information includes information about online endpoints. When an online endpoint registers with or unregisters from the master LifeSize Gatekeeper, the master LifeSize Gatekeeper automatically updates the slave LifeSize Gatekeeper via the reliable TCP/IP channel established through the Inter-gatekeeper Communication Port.

Routing Mode

The **Routing mode** field in the **Calls** section of the **Settings** tab affects what happens to a call when the Primary LifeSize Gatekeeper goes offline and is replaced by the Secondary LifeSize Gatekeeper:

- In **Direct** Mode an existing call remains connected. A direct call in mid-Setup will be disconnected when the Primary LifeSize Gatekeeper goes offline.
- In **Call Setup (Q.931)** Mode or **Call Setup (Q.931) and Call Control (H.245)** Mode, a call in mid-Setup when the Primary LifeSize Gatekeeper goes offline will be disconnected. A call in progress when the Q.931 TCP connection fails will usually be disconnected, but may be reconnected depending on endpoint capabilities.

IP Release

IP Release is a standalone service that runs in parallel with every LifeSize Gatekeeper. IP Release prevents IP address conflicts by releasing the LifeSize Gatekeeper Public IP address when it recognizes that some LifeSize Gatekeeper service has gone offline.

Configuring the Alternate Gatekeeper Function

This section describes the configuration options in the **Alternate Gatekeeper** section of the **Settings** tab.

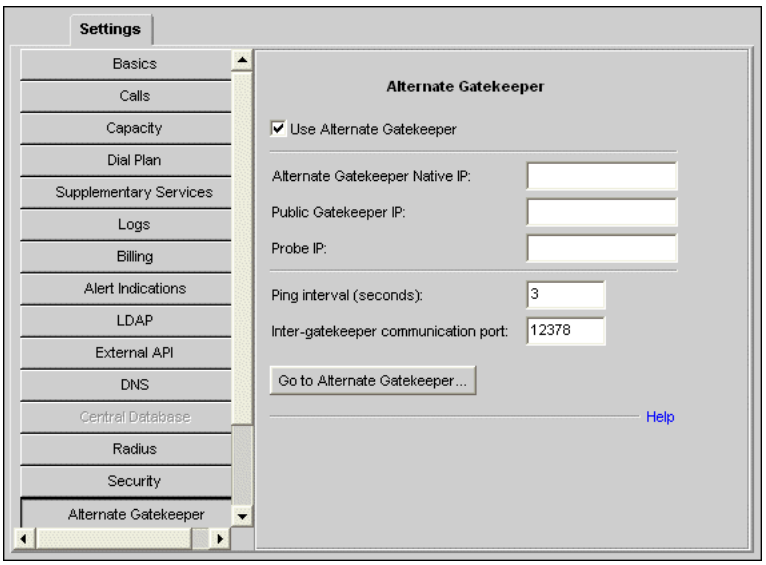

Figure 5-22 *Settings Tab: Alternate Gatekeeper*

What You Can Configure

The following options are available for configuring the **Alternate Gatekeeper** settings:

Use Alternate Gatekeeper

Check in both the Primary LifeSize Gatekeeper and the Secondary LifeSize Gatekeeper to enable the two LifeSize Gatekeepers to work in an Alternate Gatekeeper environment.

Alternate Gatekeeper Native IP

In the Primary LifeSize Gatekeeper, enter the Native IP address of the Secondary LifeSize Gatekeeper. In the Secondary LifeSize Gatekeeper, enter the Native IP address of the Primary LifeSize Gatekeeper.

Public Gatekeeper IP

Enter the Public Gatekeeper IP address. You must configure the Primary LifeSize Gatekeeper and the Secondary LifeSize Gatekeeper with the same Public Gatekeeper IP address.

To enable the Alternate Gatekeeper feature, all endpoints must register to the Public Gatekeeper IP address. This IP address should also be known to all Parent, Neighbor and Child Gatekeepers.

Probe IP

Enter the Probe IP address. This is the IP address which the LifeSize Gatekeeper pings to check that it is properly connected to the network.

Ping interval (seconds)

Enter the time interval (in seconds) at which the slave LifeSize Gatekeeper checks the status of its connection to the master LifeSize Gatekeeper.

Inter-gatekeeper communication port

Enter the number of the port through which the Primary LifeSize Gatekeeper and the Secondary LifeSize Gatekeeper communicate with each other. The default port number is 12378.

Go to Alternate Gatekeeper

Click the **Go to Alternate Gatekeeper** button to open the LifeSize Gatekeeper Administrator **Login** screen to view or configure settings in the Alternate Gatekeeper.

ADVANCED

The **Advanced** section of the **Settings** tab allows you to configure various advanced settings.

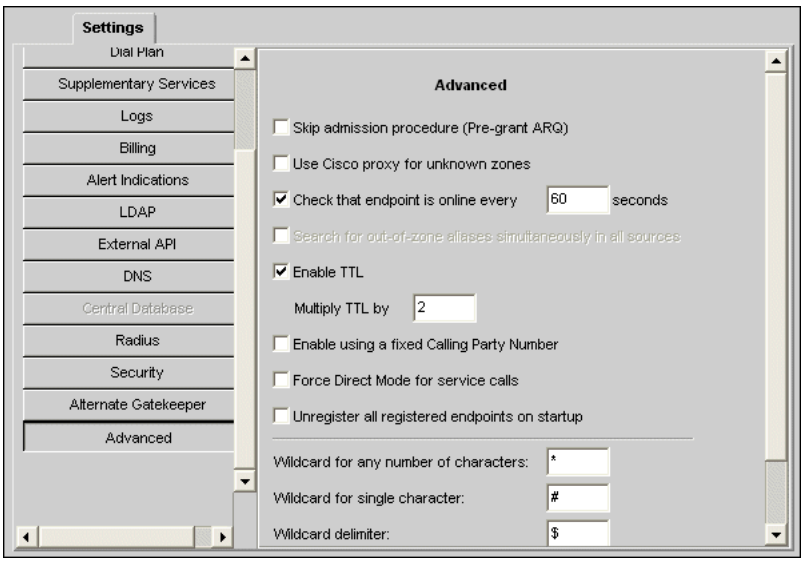

Figure 5-23 *Settings Tab: Advanced*

WHAT YOU CAN CONFIGURE

The following options are available for configuring the **Advanced** settings:

Skip admission procedure (Pre-grant ARQ)

When checked, all endpoints in the LifeSize Gatekeeper zone have pre-granted permission when they make an admission request to the LifeSize Gatekeeper. This enables faster Call Setup in environments where admission is guaranteed through means other than the Admissions Request/Admissions Confirm (ARQ/ACF) exchange.

Use Cisco proxy for unknown zones

Select this option to specify that all calls for unknown zones must be routed via the Cisco Proxy. For more information about the Cisco Proxy, see Cisco Proxy Support on page 6.

Check that endpoint is online every *n* seconds

The LifeSize Gatekeeper uses the H.323 polling mechanism which works with Information Request/Information Request Response (IRQ/IRR) messages. Enter an IRQ interval value in seconds to control the frequency with which the LifeSize Gatekeeper sends an IRQ message to each online dynamically registered endpoint to verify that it is still online. The LifeSize Gatekeeper checks the activity of all endpoints listed as *Online* in the **Endpoints** section of the **Endpoints** tab. For more information, see the Endpoints Tab chapter.

Warning Using the **Check that endpoint is online every n seconds** option with endpoints that do not support IRQ messages causes operational problems such as call disconnect.

When you set the IRQ interval you should take the following into account:

- IRQ messages increase network traffic.
- A shorter delay means more IRQ messages, but a longer delay means that it will take longer for the LifeSize Gatekeeper to detect that a dynamic endpoint is no longer online.
- The delay relates to the interval between two IRQ messages per endpoint. The actual number of IRQ messages that the LifeSize Gatekeeper creates during the interval is a multiple of all the endpoints registered dynamically.
- An active endpoint replies to an IRQ message with an IRR message. If the LifeSize Gatekeeper does not receive an IRR message, the LifeSize Gatekeeper unregisters the endpoint in question.

Search for out-of-zone aliases simultaneously in all sources

When checked, instructs the LifeSize Gatekeeper to resolve unrecognized aliases via the following methods simultaneously:

- Searching in the LDAP server.
- Searching in a DNS server.
- Searching among the Neighbor Gatekeepers that appear in the **Neighbors** tab when the **Dial Plan** field in the **Basics** section of the **Settings** tab is set to **Version 1**.
- Using multicast.

Note This option is disabled when **Version 2** is selected in the **Dial Plan version** field in the **Basics** section of the **Settings** tab.

For more information about the LRQ policy of the LifeSize Gatekeeper, see Resolution of Aliases on page 9.

Enable TTL

When checked, a registered endpoint must re-register with the LifeSize Gatekeeper when the endpoint TTL expires.

If the endpoint does not re-register, the LifeSize Gatekeeper assumes that the endpoint has gone offline when the endpoint TTL expires, and the LifeSize Gatekeeper unregisters the endpoint.

When unchecked, the LifeSize Gatekeeper ignores the endpoint TTL setting and regards that endpoint as being online, even after the endpoint TTL setting expires.

Multiply TTL by *n*

Enables an administrator to increase the length of time that the LifeSize Gatekeeper waits for a TTL before an endpoint is unregistered. Type an integer between 1 and 100 to indicate the factor by which you want to multiply the TTL value in the endpoint. The default setting is 2.

The length of time that the LifeSize Gatekeeper waits for a TTL before unregistering an endpoint is determined as follows:

```
(value entered in Multiply TTL by n option) * (endpoint TTL)
+ 20 seconds
```

This option is enabled only when you check the **Enable TTL** field. When enabled, you must enter a value for this option.

Note If you modify either the **Enable TTL** setting or the **Multiply TTL by *n*** value after an endpoint has registered to the LifeSize Gatekeeper, the LifeSize Gatekeeper implements the new values only after the endpoint re-registers.

Enable using a fixed Calling Party Number

Check to enable the Fixed Calling Party Number feature.

Note The Fixed Calling Party Number feature is enabled only when either the **Call Setup (Q.931)** option or the **Call Setup (Q.931) and Call Control (H.245)** option is selected in the **Routing mode** field in the **Calls** section of the **Settings** tab. For more information about routing modes, see Routing mode on page 51.

For more information about the Fixed Calling Party Number feature, see Fixed Calling Party Number on page 13, Configuring a Fixed Calling Party Number Alias on page 53 and Adding or Modifying a Predefined Endpoint on page 130.

Note When the **Enable using a fixed Calling Party Number** field is checked, the **Use as Calling Party Number** indicator appears in the **Aliases** list in the **Predefined Endpoint Properties** dialog box in the **Endpoints** section of the **Endpoints** tab, and the **Always use as Calling Party Number** field appears in the **Add Alias** and **Edit Alias** dialog boxes accessed via the **Predefined Endpoint Properties** dialog box. For more information, see Configuring a Fixed Calling Party Number Alias on page 53 and Adding or Modifying a Predefined Endpoint on page 130.

Force Direct Mode for service calls

When unchecked, the LifeSize Gatekeeper automatically switches to Routed Mode when processing calls to a service (such as a gateway or LifeSize Multipoint), even if the LifeSize Gatekeeper is configured to work in Direct Mode. For more information about routing modes, see Routing mode on page 51.

Note The **Force Direct Mode for service calls** field is enabled only when the **Direct** option is selected in the **Routing mode** field in the **Calls** section of the **Settings** tab. For more information about routing modes, see Routing mode on page 51.

Warning Do not use the **Force Direct Mode for service calls** option when using the LifeSize Gatekeeper with a LifeSize Multipoint or a LifeSize Gateway, since **Force Direct Mode for service calls** prevents Line or Conference Hunting operating properly.

Unregister all registered endpoints on startup

Check to clear the LifeSize Gatekeeper database of all registrations on startup. Checking this option instructs the LifeSize Gatekeeper to send unregistration messages to all the endpoints in the LifeSize Gatekeeper database. The endpoints are forced to update their registration. Unchecked by default.

Wildcard for any number of characters

Type a wildcard character for use in Forwarding Rules that apply to any dialed string of any number of digits. For example, using an asterisk (*) to forward all calls to destination number 123 functions as shown in Table 5-3.

Table 5-3 Wildcard Forwarding Rule Examples—Any Character

Forwarding Rule	Dialed Number	Forwarded To
* becomes 123	5678	123
* becomes 123	5500403	123
* becomes 123	605708	123

Wildcard for single character

Type a wildcard character for use in Forwarding Rules that apply to a single specified character within a dialed string. For example, using a question mark (?) to forward all calls containing the destination number 90?1 to the revised destination number 9001 functions as shown in Table 5-4.

Table 5-4 Wildcard Forwarding Rule Examples—Single Character

Forwarding Rule	Dialed Number	Forwarded To
90?1 becomes 9001	9011	9001
90?1 becomes 9001	9021	9001
90?1 becomes 9001	9061	9001

Wildcard delimiter

Type a wildcard character for use as a delimiter in Forwarding Rules that apply to the *callerId* field within H.323 messages. For example, using a dollar sign ($) as a delimiter for the H.323 *callerId* field functions as shown in Table 5-5 where the specified call identifier is 138.

Table 5-5 Wildcard Forwarding Rule Examples—Delimiter

Forwarding Rule	Dialed Number	Forwarded To
9013 becomes $callerId$9023	9013	1389023
8013 becomes $callerId$9055	8013	1389055

Remember Wildcard Forwarding enables the LifeSize Gatekeeper to manipulate the incoming call source number *before* searching for the destination endpoint. You configure Forwarding Rules in the **Forwarding** section of the **Forwarding/Fallback** tab.

6

NEIGHBORS TAB

ABOUT NEIGHBOR GATEKEEPERS

Neighbor Gatekeepers is a mechanism by which the LifeSize Gatekeeper optimizes inter-zone communication. Neighbor Gatekeepers are stored in a Neighbor Table in the LifeSize Gatekeeper database. The LifeSize Gatekeeper uses this table for resolving destination IP addresses when the source endpoint is not in the same zone as the destination endpoint.

The list of Neighbor Gatekeepers and their IP addresses allows a gatekeeper to search for and communicate directly with the gatekeeper of the destination endpoint. As a result, there is no need for a gatekeeper to multicast a Location Request message (LRQ) to the entire network in order to resolve addresses from other zones. This makes call routing to the other zones more efficient and reliable.

To define Neighbor Gatekeepers, you specify the IP address and port number of the Neighbor Gatekeeper. You can also specify a zone prefix. Each Neighbor Gatekeeper should have a unique prefix. If you specify a zone prefix, the LifeSize Gatekeeper routes LRQ messages and calls only to the Neighbor Gatekeeper that starts with the zone prefix in the destination address.

Note You can configure up to a maximum of 200 Neighbor Gatekeepers.

About the Neighbors Tab

The **Neighbors** tab enables you to view, configure and modify Neighbor Gatekeepers.

Note Setting the **Dial Plan** field in the **Basics** section of the **Settings** tab to **Version 2** replaces the **Neighbors** tab with the **Hierarchy** tab and opens the **Services** and **Global Services** sections of the **Services** tab. For more information about the **Hierarchy** tab, see the Hierarchy Tab chapter.

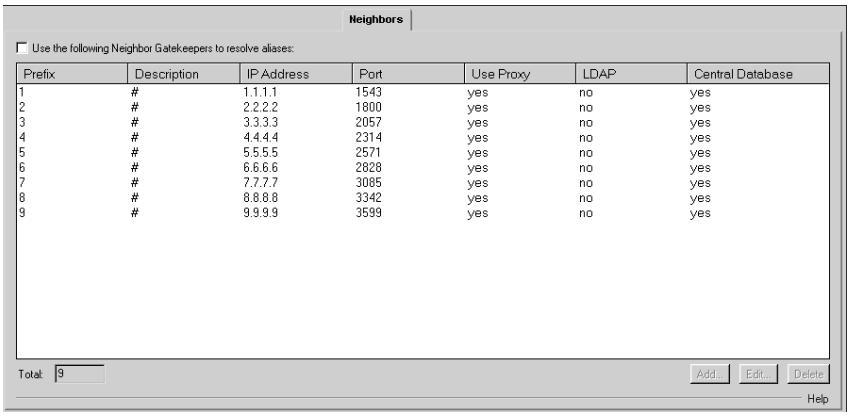

Figure 6-1 *Neighbors Tab*

What You See

The following information is displayed in the **Neighbors** tab.

Note When the **Connect to LDAP server** option is checked in the **LDAP** section of the **Settings** tab or the **Use Central Database** option is checked in the **Central Database** section of the **Settings** tab, Neighbor Gatekeeper information is read-only. For more information, see LDAP on page 71 and Central Database on page 87.

Use the following Neighbor Gatekeepers to resolve aliases

Check this option to instruct the LifeSize Gatekeeper to resolve aliases by sending a Location Request message (LRQ) to the Neighbor Gatekeepers currently listed in the LifeSize Gatekeeper database. For more information about the LRQ policy of the LifeSize Gatekeeper, see Resolution of Aliases on page 9.

Table 6-1 *Neighbors Tab Configuration*

Field	Description
Prefix	Displays the zone prefix. For information on zone prefixes, see Zone Prefix 1 and 2 Service on page 157.
Description	Displays the Neighbor Gatekeeper description in free text.
IP Address	Displays the IP address of the Neighbor Gatekeeper.
Port	Displays the port number of the Neighbor Gatekeeper.
Use Proxy	Indicates whether or not the LifeSize Gatekeeper routes all calls from this zone to the Neighbor Gatekeeper through the Cisco Proxy. For more information about the Cisco Proxy, see Cisco Proxy Support on page 6.
LDAP	Indicates whether or not the Neighbor Gatekeeper was retrieved from the LDAP server. For information on the LDAP server, see LDAP on page 71.
Central Database	Indicates whether or not the Neighbor Gatekeeper was retrieved from the Central Database. For information on the Central Database, see Central Database on page 87.

Total

The total number of Neighbor Gatekeepers currently listed in the LifeSize Gatekeeper database.

What You Can Configure

Add

Click to add a Neighbor Gatekeeper to the LifeSize Gatekeeper database. For more information, see Adding or Modifying a Neighbor Gatekeeper on page 114.

Edit

Double click the relevant Neighbor Gatekeeper in the list, or select a Neighbor Gatekeeper and click **Edit** to modify a Neighbor Gatekeeper. For more information, see Adding or Modifying a Neighbor Gatekeeper on page 114.

Delete

Select a Neighbor Gatekeeper and click the **Delete** button to delete the selected Neighbor Gatekeeper from the LifeSize Gatekeeper database.

Note The **Add**, **Edit** and **Delete** options are disabled when you check the **Connect to LDAP server** option in the **LDAP** section of the **Settings** tab or the **Use Central Database** option in the **Central Database** section of the **Settings** tab.

Adding or Modifying a Neighbor Gatekeeper

To add a new Neighbor Gatekeeper, click **Add** to display the **Add Neighbor** dialog box. To modify an existing Neighbor Gatekeeper, double click the required Neighbor Gatekeeper in the **Neighbors** tab, or select a Neighbor Gatekeeper and click **Edit** to display the **Edit Neighbor** dialog box.

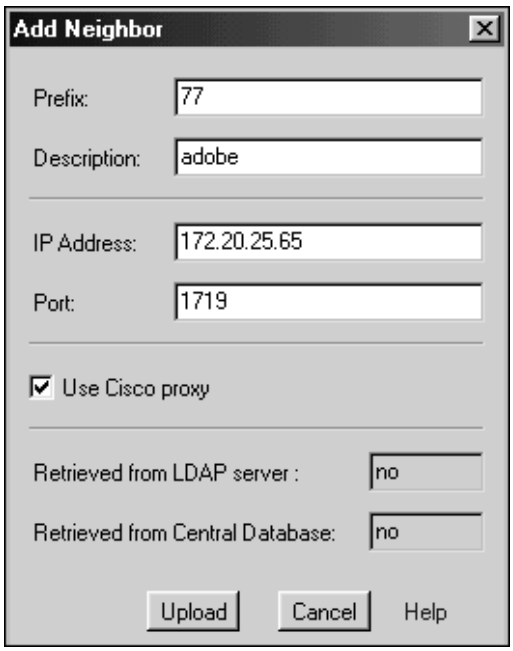

Figure 6-2 *Add Neighbor Dialog Box*

The following options are available in the **Add Neighbor** and **Edit Neighbor** dialog box:

Prefix

Type or modify the Neighbor Gatekeeper zone prefix. For information on zone prefixes, see Zone Prefix 1 and 2 Service on page 157.

Description

Type or modify the description of the Neighbor Gatekeeper.

IP Address

Type or modify the IP address of the Neighbor Gatekeeper.

Port

Type or modify the port number of the Neighbor Gatekeeper.

Use Cisco proxy

Select this option to specify whether or not the LifeSize Gatekeeper should route all calls from this zone to the Neighbor Gatekeeper through the Cisco Proxy. For more information about the Cisco Proxy, see Cisco Proxy Support on page 6.

Retrieved from LDAP server (read only)

Indicates whether or not the Neighbor Gatekeeper was retrieved from the LDAP server. The configuration of Neighbor Gatekeepers retrieved from the LDAP server should be done through configuration of the information stored in the LDAP server and not through information stored in the LifeSize Gatekeeper. For more information on the LDAP server, see LDAP on page 71 and the Configuring the LDAP Server chapter.

Retrieved from Central Database (read only)

Indicates whether or not the Neighbor Gatekeeper was retrieved from the Central Database.

Upload

Click the **Upload** button to add the Neighbor Gatekeeper to the LifeSize Gatekeeper database.

7

REGISTRATION RESTRICTIONS TAB

ABOUT THE REGISTRATION RESTRICTIONS TAB

The **Registration Restrictions** tab enables you to view and configure registration restriction information. Restricting endpoint registrations reduces the chance of non-authorized endpoints accessing the LifeSize Gatekeeper. You can define different restriction rules for an endpoint according to two options:

- Alias Format
- IP Subnet

Note Registration restrictions are not valid when the LifeSize Gatekeeper works with a LifeSize Gateway and LifeSize Multipoint.

ALIAS FORMAT

The **Alias Format** section of the **Registration Restrictions** tab enables you to define rules for specifying the allowed length of the endpoint E.164 alias with which the LifeSize Gatekeeper permits an endpoint to register.

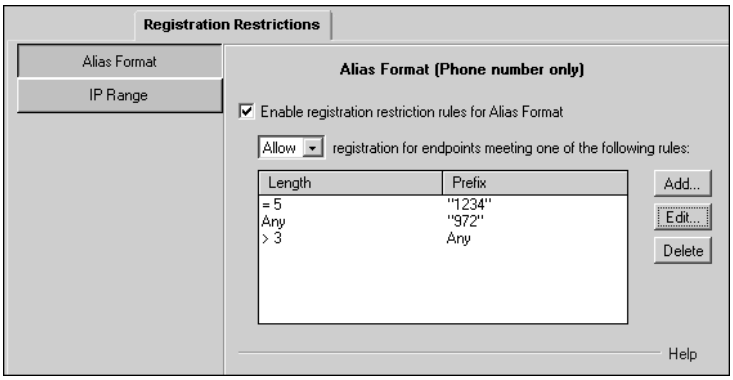

Figure 7-1 *Registration Restrictions Tab: Alias Format*

WHAT YOU SEE AND CAN CONFIGURE

The following information is displayed in the **Alias Format** section of the **Registration Restrictions** tab:

Enable registration restriction rules for Alias Format

When checked, enables you to configure and apply new Alias Format rules, and to apply existing Alias Format rules to the LifeSize Gatekeeper.

... registration for endpoints meeting one of the following rules

Select **Allow** or **Deny** from the drop-down list to define your Alias Format rule policy. Selecting **Allow** enables an endpoint to register, provided the endpoint satisfies at least one of the defined rules. Selecting **Deny** prevents an endpoint from registering even if the endpoint satisfies only one of the defined rules.

Table 7-1 *Registration Restrictions Tab: Alias Format Configuration*

Field	Description
Length	Displays the length restriction for the endpoint E.164 alias.
Prefix	Displays the prefix restriction for the endpoint E.164 alias.

Note A rule consists of both a length value and a prefix value.

Add

Click to add an Alias Format rule to the LifeSize Gatekeeper database. You can define up to five rules. For more information, see Adding or Modifying an Alias Format Rule on page 120.

Edit

Double click an Alias Format rule in the list, or select an Alias Format rule and click **Edit** to modify the selected Alias Format rule. For more information, see Adding or Modifying an Alias Format Rule on page 120.

Delete

Click to delete the selected Alias Format rule from the LifeSize Gatekeeper database.

Adding or Modifying an Alias Format Rule

To add an Alias Format rule to the LifeSize Gatekeeper database, click **Add** to display the **Add Alias Format Rule** dialog box. To modify an existing Alias Format rule in the LifeSize Gatekeeper database, select the required rule and click **Edit**, or double click the required rule to display the **Edit Alias Format Rule** dialog box.

The following options are available in the **Add Alias Format Rule** and **Edit Alias Format Rule** dialog box:

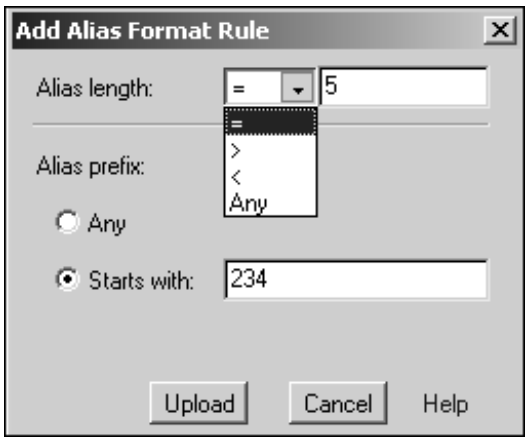

Figure 7-2 *Add Alias Format Rule Dialog Box*

Alias length

Select the required condition from the drop-down list (equal to, greater than, less than or any) and enter the required length (in characters) of the endpoint E.164 alias. Selecting **Any** instructs the LifeSize Gatekeeper to accept a prefix of any length. The length value must be from 1 to 256.

Alias prefix

Select **Any** or **Starts with** to indicate the prefix of the endpoint E.164 alias. The prefix must contain at least one digit. Selecting **Any** instructs the LifeSize Gatekeeper to accept any prefix. The length of the prefix (in characters) cannot exceed the length of the alias defined in the **Alias length** field.

Note A rule with both the **Alias length** and **Alias prefix** fields set to **Any** is invalid. Such a rule allows all E.164 aliases with no restriction.

Upload

Click to add the Alias Format rule to the LifeSize Gatekeeper database. You can define up to five rules.

IP SUBNET

The **IP Subnet** section of the **Registration Restrictions** tab enables you to define rules for specifying the range of IP addresses with which the LifeSize Gatekeeper allows an endpoint to register.

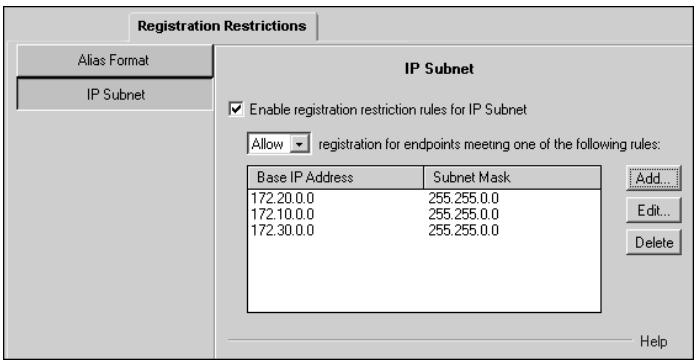

Figure 7-3 *Registration Restrictions Tab: IP Subnet*

WHAT YOU SEE AND CAN CONFIGURE

The following information is displayed in the **IP Subnet** section of the **Registration Restrictions** tab:

Enable registration restriction rules for IP Subnet

When checked, enables you to configure and apply new IP Subnet rules, and to apply existing IP Subnet rules to the LifeSize Gatekeeper.

... registration for endpoints meeting one of the following rules

Select **Allow** or **Deny** from the drop-down list to define your IP Subnet rule policy. Selecting **Allow** enables an endpoint to register, provided the endpoint satisfies at least one of the defined rules. Selecting **Deny** prevents an endpoint from registering if the endpoint satisfies at least one of the defined rules.

Table 7-2 Registration Restrictions Tab: IP Subnet Configuration

Field	Description
Base IP Address	Displays the base IP address of the IP range.
Subnet Mask	Displays the subnet mask of the endpoint.

Note The IP address and the subnet mask combine to express an IP range. For information about expressing a valid IP range, see:

http://www.microsoft.com/windows2000/en/server/help/default.asp?url=/windows2000/en/server/help/sag_RRAS-Ch1_89.htm.

Add

Click to add an IP Subnet rule to the LifeSize Gatekeeper database. You can define up to five ranges. For more information, see Adding or Modifying an IP Subnet Rule on page 122.

Edit

Double click an IP Subnet rule in the list, or select an IP Subnet rule and click **Edit** to modify the selected IP Subnet rule. For more information, see Adding or Modifying an IP Subnet Rule on page 122.

Delete

Click to delete the selected IP Subnet rule from the LifeSize Gatekeeper database.

Adding or Modifying an IP Subnet Rule

To add an IP Subnet rule to the LifeSize Gatekeeper database, click **Add** to display the **Add IP Subnet Rule** dialog box. To modify an existing IP Subnet rule in the LifeSize Gatekeeper database, select the required rule and click **Edit,** or double click the required rule to display the **Edit IP Subnet Rule** dialog box.

The following options are available in the **Add IP Subnet Rule** and **Edit IP Subnet Rule** dialog box:

Base IP Address

Type the base IP address of the IP subnet.

Subnet mask

Type the endpoint subnet mask.

Upload

Click to add the IP Subnet rule to the LifeSize Gatekeeper database. You can define up to five ranges.

8

ENDPOINTS TAB

ABOUT THE ENDPOINTS TAB

The **Endpoints** tab enables you to view information about endpoints that are predefined and online (registered), and to configure endpoints into groups. The **Endpoints** tab includes the following sections:

- Endpoints
- Groups

ABOUT PREDEFINED ENDPOINTS

A group of endpoints together with their gatekeeper constitute a zone. You can configure a zone by predefining endpoints that are entitled to register with the LifeSize Gatekeeper. For information on registration policies, see Basics on page 46.

When you predefine an endpoint, the LifeSize Gatekeeper permanently stores the predefined properties in the LifeSize Gatekeeper database. This means that the predefined information is available even if the endpoint is not registered.

When an endpoint registers with the LifeSize Gatekeeper, it is active and ready to receive calls. Even if it is not predefined, any endpoint can register with the LifeSize Gatekeeper and conduct a Discovery and Registration procedure provided that **Everyone** is selected in the **Who can register** field of the **Basics** section of the **Settings** tab.

The benefits of predefining endpoints are:

- When you choose a strict zone policy, by predefining an endpoint you can define the subset of endpoints that is allowed to register.

Note LifeSize recommends that you use groups to perform this function. For more information, see Groups on page 140.

- When you choose an open zone policy, by predefining an endpoint you give the endpoint special attributes. For example, when you edit the service permission of an endpoint, you can specify to which services this endpoint has permission and to which services access is prohibited.
- In DHCP mode only aliases identify an endpoint. Two endpoints can register using the same IP address and different ports without predefining this information provided that the two endpoints have different aliases.
- Predefined endpoints enable the LifeSize Gatekeeper to support endpoints that do not support RAS. You can predefine aliases for these endpoints and indicate that the endpoints should be treated as if they were dynamically registered. The LifeSize Gatekeeper stores the aliases and routes calls to these endpoints.

ENDPOINTS

The **Endpoints** section of the **Endpoints** tab enables you to select an endpoint and update its predefined properties or view its registered properties. You can also add or remove predefined endpoints, and unregister a selected endpoint or all endpoints.

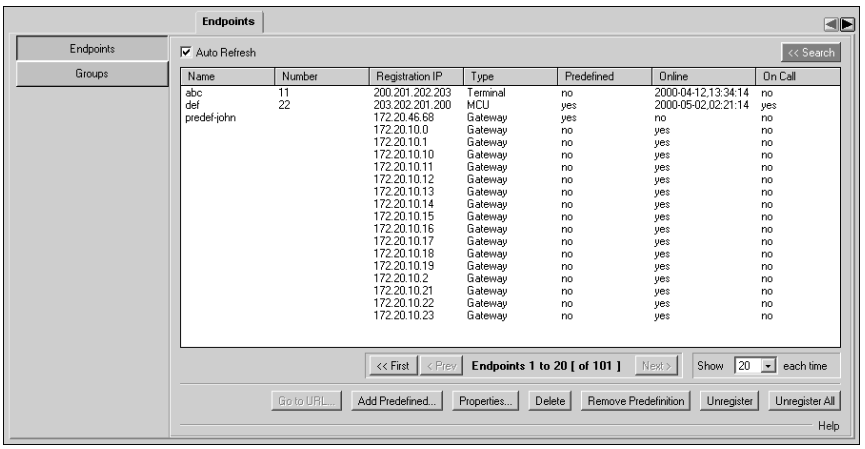

Figure 8-1 *Endpoints Tab: Endpoints*

WHAT YOU SEE

The following information is displayed in the **Endpoints** section of the **Endpoints** tab:

Auto Refresh

When checked, the LifeSize Gatekeeper checks whether or not the information in the **Endpoints** section of the **Endpoints** tab has changed at predetermined intervals of ten seconds. Any changes are updated automatically to the **Endpoints** section.

Table 8-1 *Endpoints Tab: Endpoints Configuration*

Field	Description
Name	Displays the H.323 alias name of the endpoint. Where an endpoint has more than one alias, only the first one is displayed.
Number	Displays the E.164 alias number of the endpoint. Where an endpoint has more than one alias, only the first one is displayed.

Table 8-1 *Endpoints Tab: Endpoints Configuration*

Field	Description
Registration IP	Displays the IP address of the endpoint.
Type	Displays the type of endpoint—terminal, MCU or gateway.
Predefined	Indicates whether or not the endpoint has been predefined.
Online	Indicates whether or not the endpoint is registered.
On Call	Indicates whether or not the endpoint is participating in the current LifeSize Gatekeeper session.

WHAT YOU CAN CONFIGURE

The following buttons are available for searching for, displaying and configuring LifeSize Gatekeeper endpoints:

Search/Close Search

Click **Search** or **Close Search** to open or close the search engine. When you close the search engine, the endpoints are displayed from the beginning of the list.

Look for endpoints where the ... is ...

Select the filter through which you want to perform the search from the drop-down list: **phone number**, **name**, **URL address**, **transport address** or **e-mail address**. Type the details of one of the above options for which you are searching. You must type the *full* alias.

Note The alias is case-sensitive.

Find

Click the **Find** button to perform the search.

First

Click the **First** button to display the first block of endpoints.

Previous

Click the **Previous** button to display the previous block of endpoints.

Next

Click the **Next** button to display the next block of endpoints.

Note Upon completing the search for an endpoint, the status bar below the list of endpoints displays **Search completed**. Otherwise, the status bar indicates which block of endpoints is displayed in the **Endpoints** section of the **Endpoints** tab, and the total number of endpoints in the LifeSize Gatekeeper database. For example, **Endpoints 1 to 20 [of 101]** indicates that the first block of 20 endpoints is displayed out of 101 endpoints in the LifeSize Gatekeeper database. When there are no endpoints registered in the LifeSize Gatekeeper database **No endpoints registered** is displayed.

Show *number of endpoints* each time

Select the number of endpoints you want to be displayed as a block of endpoints. You can display blocks of 10-200 endpoints in increments of 10.

Go to URL

Select the required endpoint from the list and click the **Go to URL** button to display the web interface of the specified endpoint.

Note This option is available only to endpoints which have a web interface, and for which the URL is defined in the *EndPointsVendorData.txt* parameters file.

Add Predefined

Click the **Add Predefined** button to predefine an endpoint. For more information, see Adding or Modifying a Predefined Endpoint on page 130.

Properties

Double click the relevant endpoint in the table, or select the endpoint from the list and click the **Properties** button to modify the details of an endpoint. You can modify the properties of online endpoints. You cannot modify the properties of predefined endpoints. For more information, see Adding or Modifying a Predefined Endpoint on page 130.

Remove Predefinition

Click the **Remove Predefinition** button to delete the predefined properties of the endpoint from the LifeSize Gatekeeper database. The endpoint remains registered with the LifeSize Gatekeeper.

Unregister

Click the **Unregister** button to unregister the endpoint selected in the **Endpoints** section of the **Endpoints** tab through H.323 procedures.

Unregister All

Click the **Unregister All** button to unregister all the endpoints in the **Endpoints** section of the **Endpoints** tab through H.323 procedures.

Adding or Modifying a Predefined Endpoint

To add a predefined endpoint, click the **Add Predefined** button to open the **Predefined Endpoint Properties** dialog box. The dialog box enables you to add a predefined endpoint to the LifeSize Gatekeeper database.

To modify a predefined endpoint, double click the relevant endpoint in the **Endpoints** section of the **Endpoints** tab or select the endpoint from the list and click the **Properties** button. The **Predefined Endpoint Properties** dialog box opens. The dialog box enables you to modify a predefined endpoint in the LifeSize Gatekeeper database.

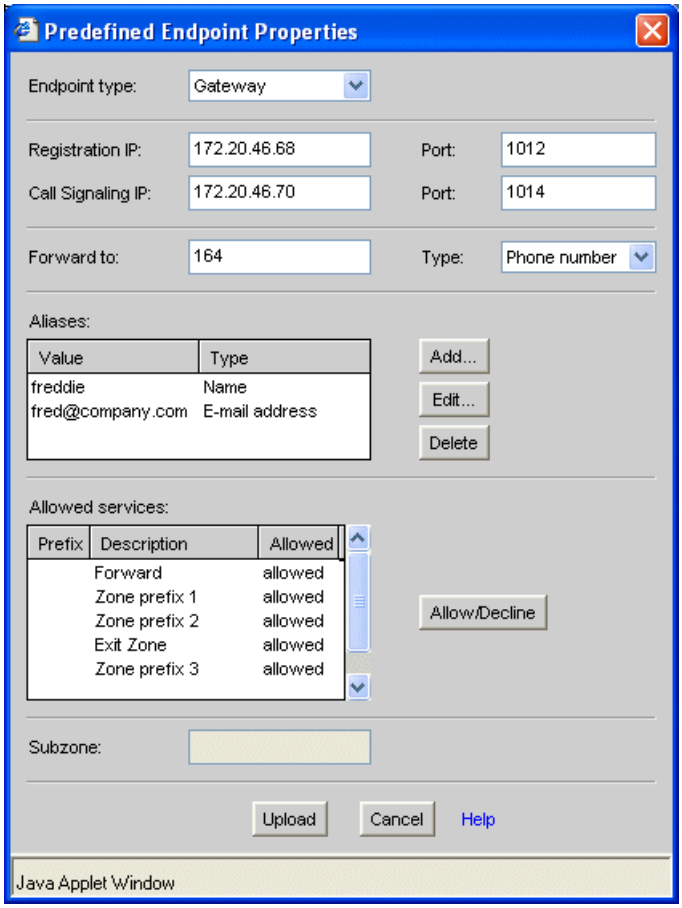

Figure 8-2 *Predefined Endpoint Properties Dialog Box*

The following options are available in the **Predefined Endpoint Properties** dialog box:

Endpoint type

Select the type of endpoint you are specifying. When an endpoint attempts to register with the LifeSize Gatekeeper, the LifeSize Gatekeeper compares the endpoint to the type that you have selected. If the type is different, the LifeSize Gatekeeper rejects the registration. If you are unsure of the type, select **Undefined**.

Registration IP

Enter or modify the registration IP address of the endpoint.

Port

Enter or modify the RAS port number of the endpoint. The default setting is 0.

Call Signaling IP

Enter or modify the Call Signaling IP address of the endpoint.

Port

Enter or modify the Call Signaling port number of the endpoint. The default setting is 0.

Note Different endpoints can be predefined with the same IP address but with different port numbers. If you do not predefine them, they must each have a unique IP address. If more than one endpoint is to run from the same computer, you must predefine each endpoint separately or use DHCP mode.

Forward to

Enter the name or number of the endpoint to which you want to forward calls that reach the endpoint you have defined. You can use this option when an endpoint does not support the H.450.3 Forwarding Supplementary Service. For more information, see Examples of the Forward Service on page 156.

Type

Select whether you want to enter either the **Name** or **Phone number** in the **Forward to** field.

Note This **Forward to** option is proprietary to LifeSize and should be differentiated from the H.450.3 Call Forwarding Supplementary Service that you add to an endpoint in the **Forwarding** section of the **Forward & Fallback** tab or define in the **Supplementary Services** section of the **Settings** tab.

ALIASES

This list displays the alias names for the endpoint.

Note When the **Enable using a fixed Calling Party Number** field in the **Advanced** section of the **Settings** tab is checked, the **Use as Calling Party Number** indicator appears in the **Aliases** section. For more information about the Fixed Calling Party Number feature, see Fixed Calling Party Number on page 13, Calls on page 50 and Advanced on page 104.

Add

Click to add an endpoint alias. For more information, see Adding or Modifying an Endpoint Alias on page 134.

Edit

Double click the relevant alias in the list, or select the relevant alias and click **Edit** to edit the selected endpoint alias. For more information, see Adding or Modifying an Endpoint Alias on page 134.

Delete

Click the **Delete** button to delete the selected endpoint alias.

ALLOWED SERVICES

This list enables you to view the LifeSize Gatekeeper services and either allow or prohibit the endpoint from using these services.

Allow/Decline

Select a service from the list and click once on this option to allow the endpoint to use this service. Click again to prohibit the endpoint from using this service.

Allowed bandwidth (Kbps) (read only)

Displays the maximum allowed bandwidth for each of the endpoints included in the group. Available only when the **Enable groups** option is checked in the Groups section of the **Endpoints** tab.

Allow making calls

Check to enable the endpoint to initiate calls. Available only when the **Enable groups** option is checked in the Groups section of the **Endpoints** tab.

Allow receiving calls

Check to enable the endpoint to receive calls. Available only when the **Enable groups** option is checked in the Groups section of the **Endpoints** tab.

Groups

Click to view the properties of the groups of which this endpoint is a member. Available only when the **Enable groups** option is checked in the Groups section of the **Endpoints** tab. For more information, see Viewing Properties of the Group to which an Endpoint Belongs on page 136.

Subzone

Displays the subzone to which the endpoint belongs, as defined in the Subzones section of the **Bandwidth Policy** tab.

Upload

Click the **Upload** button to add the predefined endpoint to the LifeSize Gatekeeper database.

Adding or Modifying an Endpoint Alias

An endpoint alias is an alternative identification string for an IP address. An alias can be a URL address, an e-mail address, a transport address in the form of "IP address:port number" or a party number. The party number is the dialing number of an endpoint which can be a telephone number or a number used by other mechanisms on various networks such as telex and ISDN.

If the alias is a party number, you must specify the type of party number. The type is the scope of the E.164 number, such as Public Unknown, Public International and Public National, as specified in the H.323 version 2 Recommendation.

To add an alias to an endpoint in the **Predefined Endpoint Properties** dialog box, click **Add** in the **Predefined Endpoint Properties** dialog box to display the **Add Alias** dialog box.

To modify an existing endpoint alias, double click the required alias in the list, or select the relevant alias and click **Edit** in the **Predefined Endpoint Properties** dialog box to display the **Modify Alias** dialog box.

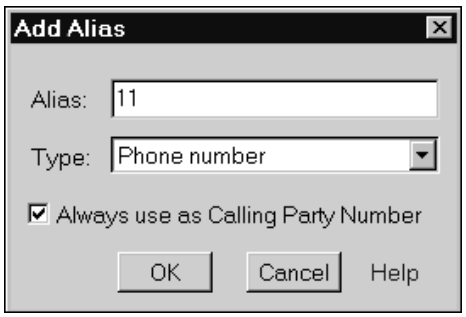

Figure 8-3 *Add Alias Dialog Box*

The following options are available in the **Add Alias** or **Modify Alias** dialog box:

Alias

Enter or modify the endpoint alias number, name, URL address, transport address (in the format “IP address: port number”), e-mail address or party number.

Type

Select the alias type. If you select **Party number**, the **Number Type** field is displayed.

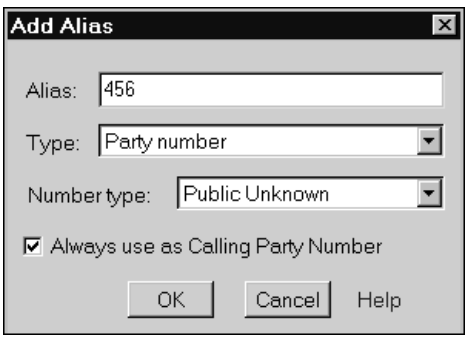

Figure 8-4 *Add Alias Dialog Box with Number Type Field*

Number type

Enter or modify the required party number type.

Always use as Calling Party Number

Check to use the new alias as the endpoint Fixed Calling Party Number. For more information about the Fixed Calling Party Number feature, see Fixed Calling Party Number on page 13 and Advanced on page 104.

Note The **Always use as Calling Party Number** field is enabled only when you select **Phone number** or **Party number** from the drop-down list in the **Type** field.

VIEWING PROPERTIES OF THE GROUP TO WHICH AN ENDPOINT BELONGS

Click the **Groups** button in the **Predefined Endpoint Properties** dialog box to display the **Endpoint Groups** dialog box.

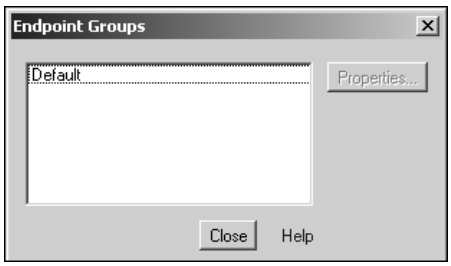

Figure 8-5 *Endpoint Groups Dialog Box*

Select the required group from the list and click **Properties** to display the **Group Properties** dialog box. The **Group Properties** dialog box displays the properties of the specified group of which the endpoint is a member.

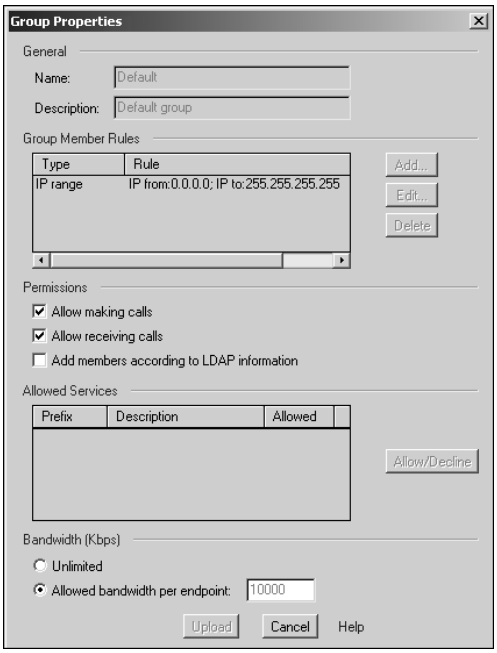

Figure 8-6 *Group Properties Dialog Box*

The following information is displayed in the **Group Properties** dialog box.

Note All displayed information is defined in the Add Group Dialog Box on page 143 in the Groups section of the **Endpoints** tab.

General

Displays the name and description of the group.

Group Member Rules

Displays the group member rules.

Permissions

Displays the permissions set for the group members.

Allowed Services

Displays the services allowed for the group members.

Bandwidth (Kbps)

Displays the bandwidth allowed for the group members.

Modifying Properties of an Online Endpoint

Double click the relevant endpoint in the **Endpoints** section of the **Endpoints** tab, or select the endpoint from the list and click the **Properties** button to open the **Online Endpoint Properties** dialog box. You can view the properties of an online endpoint and add to or modify the predefined properties of an endpoint.

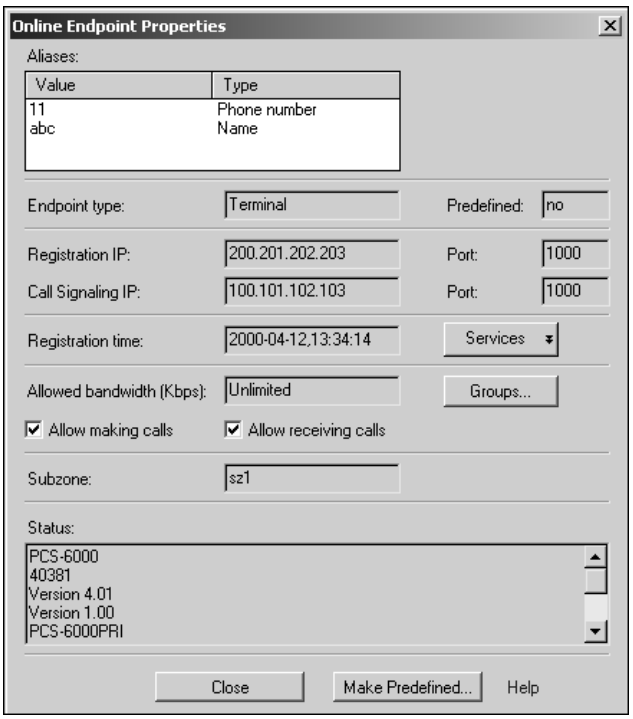

Figure 8-7 *Online Endpoint Properties Dialog Box*

The following options are available in the **Online Endpoint Properties** dialog box:

Table 8-2 *Online Endpoint Properties*

Field	Description
Aliases	A list of the alias values and types for the endpoint.
Endpoint type	The endpoint type—Gatekeeper, Gateway, MCU, Terminal or Undefined.
Predefined	Indicates whether or not the endpoint is predefined.
Registration IP	The RAS IP address of the endpoint.
Port	The RAS port number of the endpoint.
Call Signaling IP	The call signaling IP address of the endpoint.
Port	The call signaling port number of the endpoint.
Registration time	The date and time the endpoint was registered.
Allowed bandwidth (Kbps) (read only)	Displays the maximum bandwidth allowed by the group policy for each of the endpoints included in the group. If the endpoint is not part of any group, the default value (10,000 Kbps) displays. Available only when the **Enable groups** option is checked in the Groups section of the **Endpoints** tab.
Allow making calls (read only)	Displays whether or not the endpoint can initiate calls. If the endpoint is not part of any group, the default value (checked) displays. Available only when the **Enable groups** option is checked in the Groups section of the **Endpoints** tab.
Allow receiving calls (read only)	Displays whether or not the endpoint can receive calls. If the endpoint is not part of any group, the default value (checked) displays. Available only when the **Enable groups** option is checked in the Groups section of the **Endpoints** tab.
Subzone	Displays the subzone to which the endpoint belongs, as defined in the Subzones section of the Bandwidth Policy tab.

Services

Click the Services button to display the following information:

- **Supported Services**

  The services that the endpoint provides, as specified in the **Services** tab.

- **Allowed Services**

  The services that the endpoint is allowed to use, as specified in the **Services** tab.

Depending on whether or not the online endpoint is predefined, one of the **Make Predefined** or **Edit Predefined Data** options will be available for configuring online endpoints.

Groups

Click to view the properties of the groups of which this endpoint is a member. Available only when the **Enable groups** option is checked in the Groups section of the **Endpoints** tab. For more information, see Viewing Properties of the Group to which an Endpoint Belongs on page 136.

Make Predefined

Click the **Make Predefined** button to add predefined properties to an online endpoint.

Edit Predefined Data

Click the **Edit Predefined Data** button to modify the predefined properties of a specified online endpoint.

GROUPS

The **Groups** section of the **Endpoints** tab enables you to configure endpoints within groups, and to assign new services and various permissions to the endpoints included in specified groups.

ABOUT GROUPS

You allocate endpoints to groups in order to set identical service levels for all the members of a specific group. For example, you can allow all members of a defined group to initiate calls, or you can configure a single set of allowed services or a single allowed bandwidth rate within a particular group.

Note When you work with groups, configured settings override predefined endpoint settings. For example, all group services are allowed in predefined endpoints.

Every endpoint registered to the LifeSize Gatekeeper is allocated to a group according to the criteria defined for that group, and to the default group. If an endpoint does not match the criteria of any defined group, the endpoint is allocated to the default group only and will acquire the default settings of that group.

If an endpoint is a member of more than one group, the least severe of the restrictions on a particular parameter will apply. For example, an endpoint belongs to Group 1 and Group 2. The maximum bandwidth setting is 100 Kbps in Group 1, and 200 Kbps in Group 2. The 200 Kbps setting will apply to the endpoint.

Group Permissions for Local Services

Permissions for local services per group are configurable only if the service is predefined. If the service is dynamic, permissions are set according to the status of the **Automatically allow any new service to all groups** option. For more information, see Automatically allow any new service to all groups on page 142.

Group Permissions for Global Services

Global services are always predefined, therefore permissions for global services per group are configurable.

When a zone includes a global service and a device which supports this service, the service appears only once. Configuring the permissions for the service affects the service both locally and globally.

Note Blocking a global service which is supported in the zone has no effect.

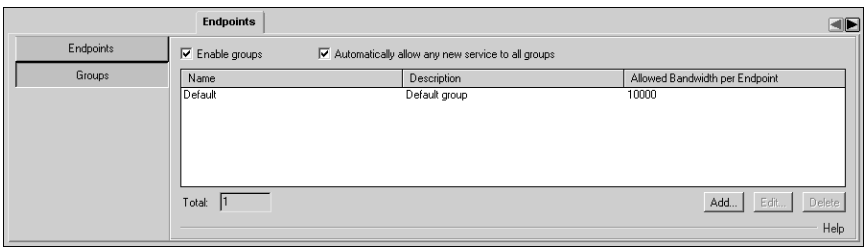

Figure 8-8 *Endpoints Tab: Groups*

What You See and Can Configure

The following information is displayed in the **Groups** section of the **Endpoints** tab:

Enable groups

Check to enable the LifeSize Gatekeeper to receive group configuration settings and to apply the groups policy.

Automatically allow any new service to all groups

Enabled only when the **Enable groups** field is checked. When checked, any new service is added automatically to the default group, thus allowing any endpoint to use this service. When unchecked, new services remain unused until manually applied to specified groups.

Table 8-3 *Endpoints Tab: Groups Configuration*

Field	Description
Name	Displays the name of the group as configured in the **Add Group** dialog box (Figure 8-9 on page 143).
Description	Displays the description of the group as configured in the **Add Group** dialog box (Figure 8-9 on page 143).
Allowed Bandwidth per Endpoint	Displays the maximum bandwidth allowed to each of the endpoints included in the group as configured in the **Add Group** dialog box (Figure 8-9 on page 143). The call is rejected if the maximum bandwidth is exceeded.

Total

Indicates the total number of groups currently listed in the LifeSize Gatekeeper database.

Add

Enabled only when the **Enable groups** field is checked. Click to add a group. For more information, see Adding or Modifying a Group on page 143.

Edit

Enabled only when the **Enable groups** field is checked. Double click the relevant group in the list, or select the required group and click **Edit** to modify the selected group. For more information, see Adding or Modifying a Group on page 143.

Delete

Enabled only when the **Enable groups** field is checked. Click to delete the selected group.

Adding or Modifying a Group

To create a new group, click **Add** to display the **Add Group** dialog box.

To modify an existing group, double click the required group in the **Groups** section of the **Endpoints** tab, or select the required group and click **Edit**. The **Edit Group** dialog box displays.

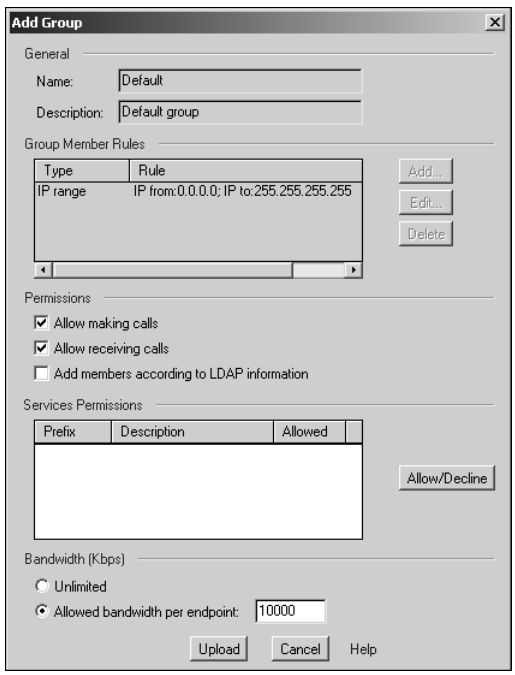

Figure 8-9 *Add Group Dialog Box*

The following options are available in the **Add Group** and **Edit Group** dialog box:

Remember When you work with groups, configured settings override predefined endpoint settings.

General

Name

Type the name of the group in free text.

Description

Type a description of the group in free text.

Endpoints

Available only for existing groups. Click to display the **Group Endpoints** dialog box. For more information, see Viewing Properties of Endpoints Belonging to a Group on page 146.

Group Member Rules

Type

Displays the property associated with the specified rule, as configured in the **Add Group Rule** dialog box. For more information, see Adding or Modifying a Group Rule on page 149.

Rule

Displays the rule configured in the **Add Group Rule** dialog box. For more information, see Adding or Modifying a Group Rule on page 149.

Add

Click to display the **Add Group Rule** dialog box. Select from the drop-down list the property associated with the specified rule and type the requested information in the fields below the drop-down list. For more information, see Adding or Modifying a Group Rule on page 149.

Edit

Double click the required group rule, or select the required group rule and click to display the **Edit Group Rule** dialog box for modifying group member rule settings. For more information, see Adding or Modifying a Group Rule on page 149.

Delete

Select a group member rule and click **Delete** to remove from the LifeSize Gatekeeper database.

Permissions

Allow making calls

Check to allow all endpoints in this group to initiate calls.

Allow receiving calls

Check to allow all endpoints in this group to receive calls.

Add members according to LDAP information

When checked, the LifeSize Gatekeeper adds a member to the group according to the service level configured in the *h323IdentityServiceLevel* attribute in the H.350 schema. For this to work, group names should match those used by the H.350 schema, such as “servicelevel”.

Note When checked, the LifeSize Gatekeeper ignores the rules of the group.

Verify that the **Add members according to LDAP information** option is unchecked in the default group.

Services Permissions

This list enables you to view the LifeSize Gatekeeper services and either allow or prohibit the endpoint from using these services.

Allow/Decline

Select a service from the list and click once on this option to allow the endpoint to use this service. Click again to prohibit the endpoint from using this service.

BANDWIDTH (KBPS)

Unlimited

Select to allow unlimited bandwidth to the specified group of endpoints.

Allowed bandwidth per endpoint

Select to configure a maximum allowed bandwidth for each of the endpoints included in the group.

VIEWING PROPERTIES OF ENDPOINTS BELONGING TO A GROUP

Click **Endpoints** to display the **Group Endpoints** dialog box. The **Group Endpoints** dialog box enables you to view details of all endpoints belonging to the specified group.

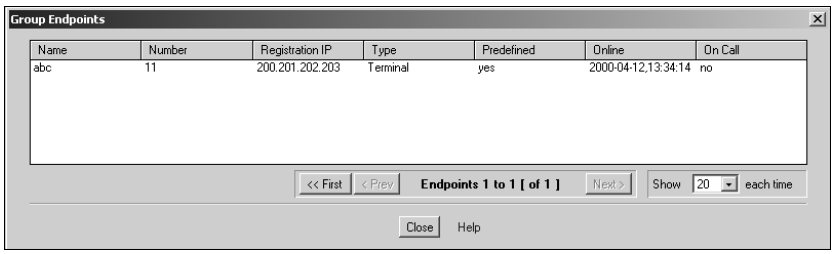

Figure 8-10 *Group Endpoints Dialog Box*

The following information is displayed in the **Group Endpoints** dialog box:

Table 8-4 *Group Endpoints Dialog Box*

Field	Description
Name	Displays the H.323 alias name of the endpoint. Where an endpoint has more than one alias, only the first one is displayed.
Number	Displays the E.164 alias number of the endpoint. Where an endpoint has more than one alias, only the first one is displayed.
Registration IP	Displays the IP address of the endpoint.
Type	Displays the type of endpoint—terminal, MCU or gateway.

Table 8-4 *Group Endpoints Dialog Box (continued)*

Field	Description
Predefined	Indicates whether or not the endpoint has been predefined.

Table 8-4 *Group Endpoints Dialog Box (continued)*

Field	Description
Online	Indicates whether or not the endpoint is registered.
On Call	Indicates whether or not the endpoint is participating in the current LifeSize Gatekeeper session.

First

Click the **First** button to display the first block of endpoints.

Previous

Click the **Previous** button to display the previous block of endpoints.

Next

Click the **Next** button to display the next block of endpoints.

Show *number of endpoints* each time

Select the number of endpoints you want to be displayed as a block of endpoints. You can display blocks of 10-200 endpoints in increments of 10.

ADDING OR MODIFYING A GROUP RULE

To add a new group rule, click **Add** to display the **Add Group Rule** dialog box.

To modify an existing group rule, double click the required group rule, or select the required group rule and click **Edit** to display the **Edit Group Rule** dialog box.

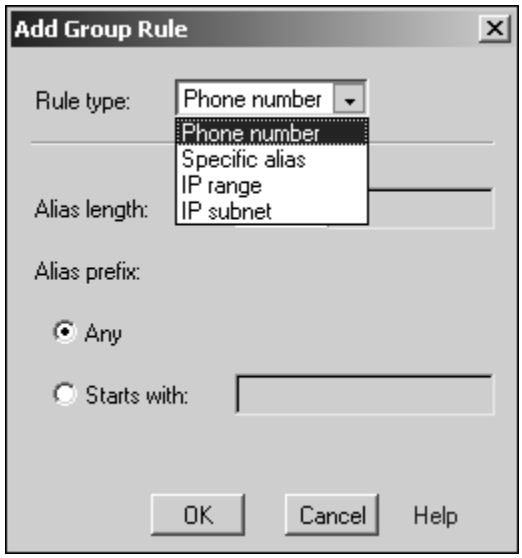

Figure 8-11 *Add Group Rule Dialog Box*

The following options are available in the **Add Group Rule** and **Edit Group Rule** dialog box:

Rule type

Select the required rule type from the drop-down list. The rule type indicates the criterion you are using to define membership of a group. The following options are available:

- **Phone number**

  Enables you to define group membership according to a specified endpoint phone number.

- **Specific alias**

  Enables you to define group membership according to a specified endpoint alias.

- **IP range**

  Enables you to define group membership according to a specified range of endpoint IP addresses.
- **IP subnet**

  Enables you to define group membership according to a specified IP subnet.

Note The available configuration options vary depending on which option you select in the Rule type field. For more information, see Options available when the Phone number rule type is selected on page 150, Options available when the Specific alias rule type is selected on page 151, Options available when the IP range rule type is selected on page 152 and Options available when the IP subnet rule type is selected on page 153.

Options available when the Phone number rule type is selected

The following options are available when the **Rule type** option is set to **Phone number**.

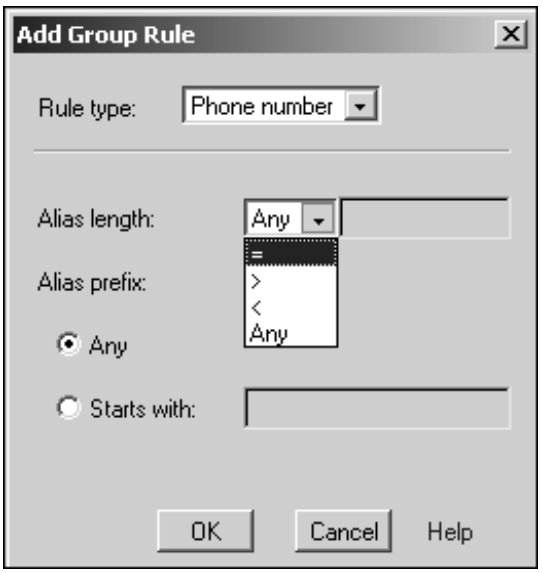

Figure 8-12 *Add Group Rule Dialog Box—Phone Number*

Alias length

Select the required condition from the drop-down list (equal to, greater than, less than or any) and enter the required length (in characters) of the endpoint E.164 alias. Selecting **Any** instructs the LifeSize Gatekeeper to accept a prefix of any length. The length value must be from 1 to 256.

Alias prefix

Select **Any** or **Starts with** to indicate the prefix of the endpoint E.164 alias. The prefix must contain at least one digit. Selecting **Any** instructs the LifeSize Gatekeeper to accept any prefix. The length of the prefix (in characters) cannot exceed the length of the alias defined in the **Alias length** field.

Note A rule with both the **Alias length** and **Alias prefix** fields set to **Any** is invalid. Such a rule allows all E.164 aliases with no restriction.

Options available when the Specific Alias rule type is selected

The following options are available when the **Rule type** option is set to **Specific Alias**.

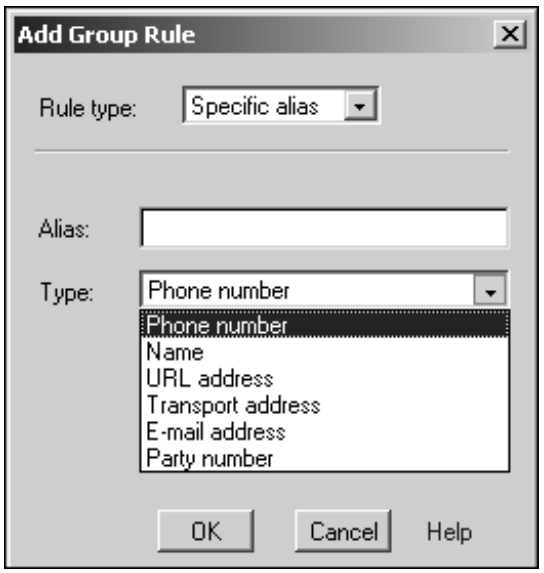

Figure 8-13 *Add Group Rule Dialog Box—Specific Alias*

Alias

Type the required alias.

Type

Select the required alias type from the drop-down list.

Options available when the IP range rule type is selected

The following options are available when the **Rule type** option is set to **IP range**.

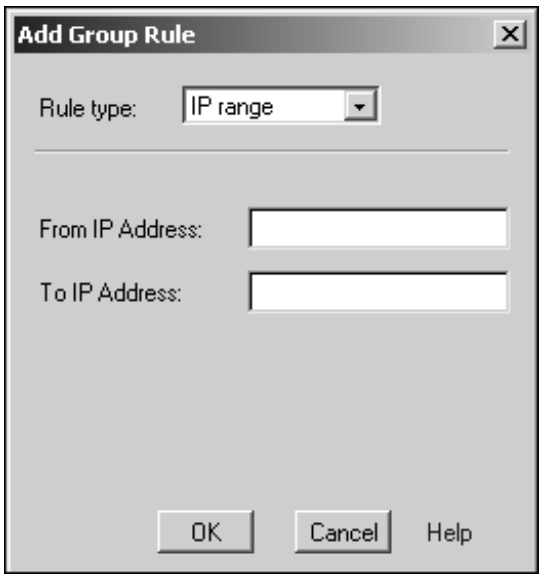

Figure 8-14 *Add Group Rule Dialog Box—IP Range*

From IP Address

Type the lower limit of the range of IP addresses between which communication through the LifeSize Gatekeeper is allowed.

To IP Address

Type the upper limit of the range of IP addresses between which communication through the LifeSize Gatekeeper is allowed.

Options available when the IP subnet rule type is selected

The following options are available when the **Rule type** option is set to **IP subnet**.

Figure 8-15 *Add Group Rule Dialog Box—IP Subnet*

Base IP Address

Type the base IP address of the IP range.

Subnet mask

Type the subnet mask.

9

SERVICES TAB

ABOUT LIFESIZE GATEKEEPER SERVICES

The LifeSize Gatekeeper supports two types of services—user-defined services that you create, and built-in services that are supplied by the LifeSize Gatekeeper. The term *user-defined services* refers both to services that are manually specified by an administrator and to those services that are dynamically specified by a gateway or an LifeSize Multipoint during registration without the intervention of an administrator. You activate an LifeSize Gatekeeper service by defining a prefix for it. You can define up to 1024 services, including built-in services, which are saved in the LifeSize Gatekeeper database. You can also define access privileges per endpoint for each service.

LifeSize Gatekeeper services are supported by a subset of endpoints in a zone—a logical collection of terminals, gateways and Multipoint Control Units (LifeSize Multipoints) managed by a single gatekeeper. At registration, an endpoint can declare support for a subset of the services defined in the zone. This is a dynamic procedure that does not involve administration.

The user accesses the service by dialing the prefix attached to the name or phone number. When the LifeSize Gatekeeper identifies that a call destination includes a prefix (service), the call is routed through the LifeSize Gatekeeper and serially accesses all endpoints providing this service until it locates an available endpoint. This is done without endpoint intervention.

Note To disable an LifeSize Gatekeeper service, remove the LifeSize Gatekeeper service prefix.

User-defined Services

User-defined services allow you to dynamically add more resources, such as a gateway, into the system. Services provide both Line Hunting and Group Hunting functionality for locating the available resources supplied via service definition. When a gateway registers, it sends a list of prefixes (services) that it supports to the LifeSize Gatekeeper. If the LifeSize Gatekeeper receives a call with one of these prefixes, it looks for the first available gateway that supports this prefix.

Built-in Services

The LifeSize Gatekeeper provides the following built-in services that you activate by giving the service a prefix:

- Forward Service
- Zone Prefix 1 and 2 Service
- Exit Zone Service

These built-in services are described below.

Forward Service

When a terminal wishes to instruct the LifeSize Gatekeeper to forward its calls, it requests the Forward service using a prefix you defined for the service together with the new destination endpoint. Subsequently, when the LifeSize Gatekeeper receives calls for that terminal, it forwards calls to the new endpoint until the terminal deactivates the Forward service request. The terminal deactivates the Forward service request by dialing the Forward prefix only.

Note The Forward service is proprietary to LifeSize and should be differentiated from the H.450.3 Forwarding Supplementary Service that you add to an endpoint in the **Forwarding** section of the **Forward & Fallback** tab or define in the **Supplementary Services** section of the **Settings** tab. You can use the LifeSize Forward service when an endpoint does not support the H.450.3 Forwarding Supplementary Service.

Examples of the Forward Service

In the examples below, note the following:

- 98* is the Forward service prefix.
- 8 is the gateway prefix for 1B or 2B calls.
- 7657333 is the number of an ISDN network terminal.
- 5318 is the number of an IP network terminal.

Example 1: Simple Forwarding of all Calls to Another IP Network Terminal

1. In the **Service Properties** window, define a prefix for the Forward service. The maximum number of characters is 64.
2. From the endpoint whose incoming calls you wish to forward, dial the Forward service prefix followed by the number of the other terminal to which you wish to forward the calls. For example, 98*5318.
3. To deactivate the Forward service, dial the Forward service prefix from the original endpoint. For example, 98*.

Example 2: Forwarding a 1B Call to Another Terminal via a Gateway

1. In the **Service Properties** window, define a prefix for the Forward service. The maximum number of characters is 64.
2. From the endpoint whose incoming calls you wish to forward, dial the Forward service prefix, the gateway prefix and the number of the other terminal. For example, 98*87657333.
3. To deactivate the Forward service, dial the Forward service prefix from the original endpoint. For example, 98*.

Zone Prefix 1 and 2 Service

You can configure the LifeSize Gatekeeper to have one or two optional zone prefixes. If the LifeSize Gatekeeper has been configured with a zone prefix, it will respond to LRQs and calls from other gatekeepers only if its zone prefix is part of the dialed number.

For example, consider a single LifeSize Gatekeeper that has been configured with a zone prefix of 6. The number of one of the endpoints in its zone is 45678. If the LifeSize Gatekeeper receives a call from another gatekeeper with the number 645678, the LifeSize Gatekeeper will strip the 6 and connect endpoint 45678 to the call. If the LifeSize Gatekeeper receives a call from outside the zone with the number 45678 it will not connect the call.

An endpoint from within the LifeSize Gatekeeper zone dialing to another endpoint in the zone does not need to dial the zone prefix. In the example, an endpoint in the zone will dial 45678 to reach endpoint 45678.

If the LifeSize Gatekeeper has not been configured with a zone prefix when performing address translation, it will not differentiate between calls from endpoints within its zone and calls from outside its zone.

Use two zone prefixes (instead of one) where two dialing plans are needed simultaneously. Since prefixes can be numeric or alphabetic, using two zone prefixes prevents ambiguity.

Example of a LifeSize Gatekeeper with Two Zone Prefixes

Consider the following scenarios:

LifeSize Gatekeeper with Dial Plan version 1 enabled

- Joe's terminal number is 1234.
- Joe's terminal is registered to LifeSize Gatekeeper A.
- LifeSize Gatekeeper A contains two zone prefixes—77 and 88.
- Tom's terminal is registered to LifeSize Gatekeeper B.

If Tom wishes to call Joe, he can dial 771234 **or** 881234.

Note In this scenario, LifeSize Gatekeeper A manages two different zone prefixes and performs stripping. All terminals registered to LifeSize Gatekeeper A must have unique numbers. The unique terminal numbers enable the LifeSize Gatekeeper to support two separate zone prefixes.

LifeSize Gatekeeper with Dial Plan version 2 enabled without stripping

- Joe's terminal number is 771234.
- Frank's terminal number is 881234
- Joe's terminal is registered to LifeSize Gatekeeper A.
- Frank's terminal is registered to LifeSize Gatekeeper A.
- LifeSize Gatekeeper A contains two zone prefixes—77 and 88.
- Tom's terminal is registered to LifeSize Gatekeeper B.

If Tom wishes to call Joe, he should dial 771234.

If Tom wishes to call Frank, he should dial 881234.

Note In this scenario, LifeSize Gatekeeper A manages two different zone prefixes without stripping.

Exit Zone Service

When you define a prefix for the Exit Zone service, dialing the prefix enables you to reach an endpoint in another zone. This can prevent unauthorized users making calls to other zones.

Note The **Exit Zone** is a historical feature introduced before the implementation of the LifeSize dial plans. The **Exit Zone** feature is no longer required but is maintained for backwards compatibility only. The **Exit Zone** service saves time by instructing the LifeSize Gatekeeper not to look for a destination within the zone, but to redirect a request to the Neighbor Gatekeeper.

The Exit Zone prefix affects the way in which the LifeSize Gatekeeper tries to complete calls to other zones. When this service is not defined, the LifeSize Gatekeeper first tries to locate any call request within its zone. The LifeSize Gatekeeper tries to locate the designated number in other zones only when the call request is not available.

When this service is defined, the LifeSize Gatekeeper completes calls to other zones if the Exit Zone prefix is present in the dialed string.

Example of Exit Zone Service Usage

1. In the **Service Properties** window, define a prefix for the Exit Zone service. For example, 06.
2. If you wish to dial a number from a terminal to another zone, dial the Exit Zone prefix and then the number. For example, 062234, where 2234 is the number of the terminal in the other zone.

About the Services Tab

The **Services** tab enables you to view, add and update service information on built-in and user-defined services.

Setting the **Dial Plan** field in the **Basics** section of the **Settings** tab to **Version 2** opens the **Services** and **Global Services** sections of the **Services** tab, and replaces the **Neighbors** tab with the **Hierarchy** tab. For more information about the **Services** and **Global Services** sections of the **Services** tab, see Services Tab in Dial Plan version 2 on page 164.

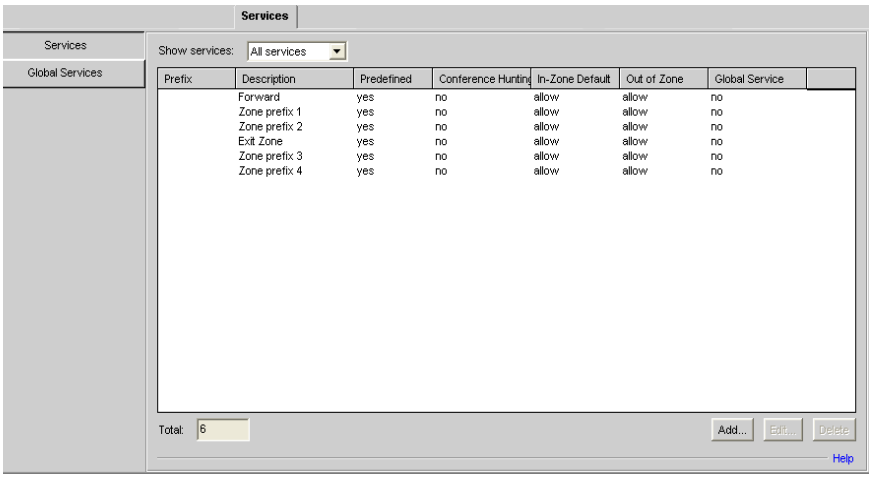

Figure 9-1 *Services Tab*

WHAT YOU SEE

To filter the entries in the list of services, select either **Predefined only** or **All services** from the **Show services** drop-down list:

The following information is displayed in the **Services** tab:

Table 9-1 *Services Tab Configuration*

Field	Description
Prefix	The prefix that identifies the service. **NOTE:** A built-in service that is defined without a prefix is disabled.
Description	The service name, as well as an indication of whether or not the service is built-in.

Table 9-1 Services Tab Configuration (continued)

Field	Description
Predefined	Indicates whether or not the LifeSize Gatekeeper service is predefined. A no indicates a LifeSize Gatekeeper service that is not predefined, meaning a gateway service that is transferred to the LifeSize Gatekeeper. A yes indicates that the service is either user-defined or built-in, and is saved in the LifeSize Gatekeeper database. If you modify a service that is not predefined, the service becomes a predefined service. **NOTE:** A service that is predefined remains in the database after all endpoints using that service have unregistered. A service that is not predefined is removed after all endpoints using that service unregister.
Conference Hunting	Defines this service as conference-oriented. A conference-oriented service lets you select one LifeSize Multipoint for a specific conference and to direct all calls that need to participate in this conference to that LifeSize Multipoint.
In-Zone Default	Indicates whether or not a service is accessible to all endpoints that are not part of the zone.
Out of Zone	Indicates whether or not the LifeSize Gatekeeper service is public and is accessible to endpoints from other zones.
Global Service	Indicates whether or not the specified service is a global service common to all gatekeepers on the network.

Total

Indicates the total number of services currently listed in the LifeSize Gatekeeper database.

WHAT YOU CAN CONFIGURE

The following options are available for configuring LifeSize Gatekeeper services:

Note The **Add**, **Edit** and **Delete** buttons are disabled for the Slave LifeSize Gatekeeper.

Add

Click to add a LifeSize Gatekeeper service. For more information, see Adding or Modifying LifeSize Gatekeeper User-Defined Services on page 162.

Edit

Double click a LifeSize Gatekeeper service in the list, or select a service and click **Edit** to modify the selected LifeSize Gatekeeper service. For more information, see Adding or Modifying LifeSize Gatekeeper User-Defined Services on page 162.

Delete

Select a service and click the **Delete** button to delete the selected LifeSize Gatekeeper service.

Adding or Modifying LifeSize Gatekeeper User-Defined Services

To add a user-defined LifeSize Gatekeeper service to the LifeSize Gatekeeper database, click **Add** to display the **Service Properties** dialog box.

To modify an existing user-defined LifeSize Gatekeeper service LifeSize Gatekeeper, double click the required service in the **Services** tab, or select the required service and click **Edit** to display the **Service Properties** dialog box. If you modify a service that is not predefined, the status of the service automatically changes to predefined. For more information on predefined endpoints, see About Predefined Endpoints in the **Endpoints** chapter.

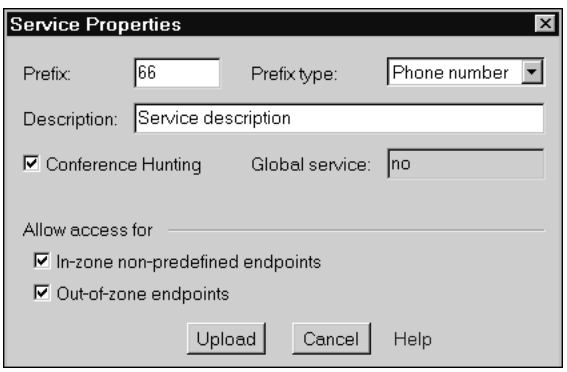

Figure 9-2 *Service Properties Dialog Box*

The following options are available in the **Service Properties** dialog box:

Prefix

Enter or modify the LifeSize Gatekeeper service prefix. The prefix can be up to 64 characters.

Prefix type

Select the type of prefix you are specifying: **Phone number**, **Name**, **URL address**, **Transport address** (in the "IP address: port number" format), **E-mail address** or **Party number**. If you select **Party number**, the **Number Type** field is displayed. For more information on Party number, see Adding or Modifying an Endpoint Alias in the **Endpoints** chapter.

Note The prefix type for a user-defined or built-in service can only be **Phone number** or **Name**. Only a gateway prefix can be of any alias type.

Description

Enter or modify the description of the LifeSize Gatekeeper service.

Conference Hunting

Defines this service as conference-oriented. A conference-oriented service lets you select one LifeSize Multipoint for a specific conference and to direct all calls that need to participate in this conference to that LifeSize Multipoint.

Global service (read only)

Indicates whether or not the specified service is a global service common to all gatekeepers on the network.

ALLOW ACCESS FOR

The **Allow access for** group box enables you determine the level of accessibility of the LifeSize Gatekeeper.

In-zone non-predefined endpoints

Select this option to make the LifeSize Gatekeeper service accessible to all endpoints that are not predefined in the zone.

Note Settings in the **Predefined Endpoint Properties** dialog box in the **Endpoints** section of the **Endpoints** tab determine which services are accessible to predefined endpoints. For more information, see Adding or Modifying a Predefined Endpoint in the **Endpoints** chapter.

Out-of-zone endpoints

Select this option to make the LifeSize Gatekeeper service public and accessible to endpoints from other zones.

Upload

Click the **Upload** button to add the LifeSize Gatekeeper service to the LifeSize Gatekeeper database. Your changes will not take effect until they are uploaded.

SERVICES TAB IN DIAL PLAN VERSION 2

Setting the **Dial Plan** field in the **Basics** section of the **Settings** tab to **Version 2** opens the **Services** and **Global Services** sections of the **Services** tab and replaces the **Neighbors** tab with the **Hierarchy** tab. The additional service features that are enabled when Dial Plan version 2 is selected are described below.

SERVICES

The **Services** section of the **Services** tab in Dial Plan version 2 is identical to the **Services** tab in Figure 9-1 on page 160.

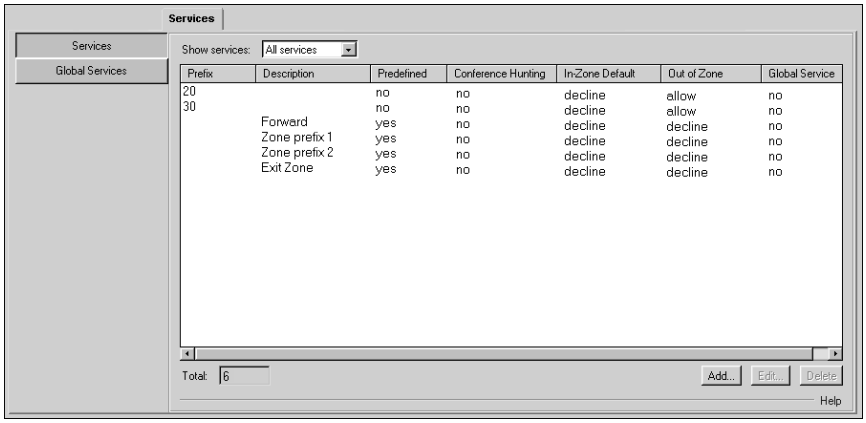

Figure 9-3 *Services Tab: Services*

GLOBAL SERVICES

The **Global Services** section of the **Services** tab enables you to view, add and update service information on global services common to all gatekeepers on the network.

ABOUT GLOBAL SERVICES

A global service is a service that is available to everyone using the network. It is identified by a universal prefix. For example, a gateway service for dialing out to the PSTN may be global with a universal prefix such as “9”. All entities in the network recognize that the prefix “9” indicates that the call should be routed to the PSTN via a gateway.

In this case, the dial string would be:

Global Service Prefix-[Zone Prefix]-endpoint number

such as:

9-1201-5294300

or *9-5294300*

Note When the **Use Central Database** option is checked in the **Central Database** section of the **Settings** tab and **Version 2** is selected in the **Dial Plan version** field in the **Basics** section of the **Settings** tab, the information displayed in the **Global Services** section is read-only. For more information about the Central Database, see the **Settings** chapter.

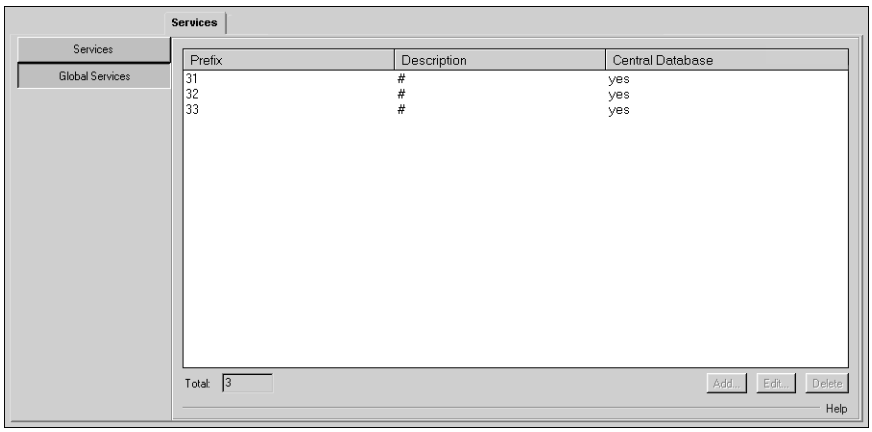

Figure 9-4 *Services Tab: Global Services*

WHAT YOU SEE

The following information is displayed in the **Global Services** section:

Table 9-2 *Global Services Configuration*

Field	Description
Prefix	The prefix that identifies the global service.
Description	The description of the global service.
Central Database	Indicates whether or not the global service has been retrieved from the Central Database.

Total

Indicates the total number of global services currently listed in the LifeSize Gatekeeper database.

What You Can Configure

The following options are available for configuring global services:

Add

Click to add a global service. For more information, see Adding or Modifying Global Services on page 167.

Edit

Double click a global service in the list, or select a global service and click **Edit** to modify the selected global service. For more information, see Adding or Modifying Global Services on page 167.

Delete

Select a service and click the **Delete** button to remove the selected global service.

Note The **Add**, **Edit** and **Delete** options are disabled when you check the **Use Central Database** option in the **Central Database** section of the **Settings** tab.

Adding or Modifying Global Services

To add a global service, click **Add** to display the **Add Global Service** dialog box. To modify an existing global service, double click the required service, or select the required service and click **Edit** to display the **Edit Global Service** dialog box.

The following options are available in the **Add Global Service** and **Edit Global Service** dialog box:

Prefix

Enter or modify the prefix that identifies the global service.

Description

Enter or modify the description of the global service.

Retrieved from Central Database

Indicates whether or not the global service has been retrieved from the Central Database.

Upload

Click the **Upload** button to add the new global service information to the Central Database.

10

BANDWIDTH POLICY TAB

ABOUT THE BANDWIDTH POLICY TAB

The **BW Policy** tab enables you to define subzones and subzone rules, and to determine bandwidth policy between zones and subzones. The **BW Policy** tab includes the following sections:

- Subzones
- Bandwidth Policy

ABOUT SUBZONES

This section describes subzones and how you can use them. A sample topology is provided in Sample Topology with Subzones on page 175.

WHAT ARE SUBZONES?

A subzone is a group of endpoints belonging to a subsection of a Gatekeeper Zone. The subzone is defined by subzone rules. Subzone rules are defined according to one of the following criteria:

- IP range
- IP subnet

For information about configuring subzone rules, see Adding or Modifying Subzone Rules on page 173.

WHY USE SUBZONES?

You can use subzone rules to control the bandwidth available between the departments of your company. You can configure a single subzone for each department including all and only the endpoints within that department. Defining appropriate subzone rules allows you to allocate a different bandwidth to connections between subzones.

Alternatively, you can use subzones to control the bandwidth available between your branch offices. Configure a single subzone for each branch office and define subzone rules that allow a different bandwidth connection per branch.

SUBZONES

The **Subzones** section of the **BW Policy** tab enables you to view and configure subzone settings and rules.

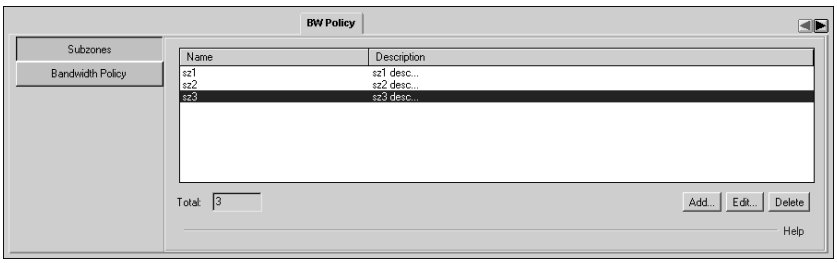

Figure 10-1 *BW Tab: Subzones*

WHAT YOU SEE

The following information is displayed in the **Subzones** section of the **BW Policy** tab:

Table 10-1 *BW Tab: Subzones Configuration*

Field	Description
Name	Displays the name of the specified subzone.
Description	Displays the description of the specified subzone.
Total	Displays the total number of subzones configured.

What You Can Configure

The following configuration options are available in the **Subzones** section of the **BW Policy** tab:

Add

Click to add a new subzone. The **Subzone Properties** dialog box displays. For more information, see Adding or Modifying Subzones on page 171.

Edit

Double click the required subzone entry in the **Subzones** section of the **BW Policy** tab, or select the required subzone entry and click **Edit** to modify an existing subzone. The **Subzone Properties** dialog box displays. For more information, see Adding or Modifying Subzones on page 171.

Delete

Select the required subzone entry in the **Subzones** section of the **BW Policy** tab and click **Delete** to remove a subzone.

Adding or Modifying Subzones

The **Subzone Properties** dialog box enables you to add a new subzone or modify existing subzone settings.

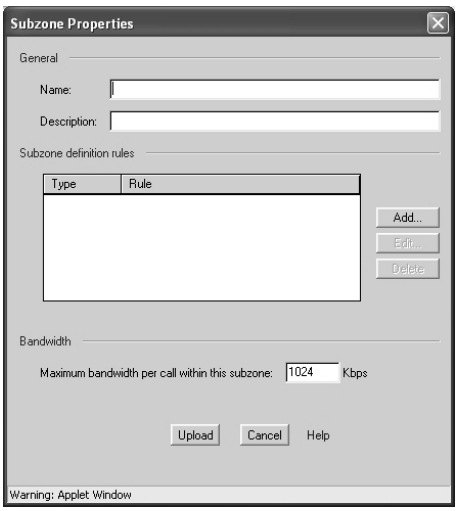

Figure 10-2 *Subzone Properties Dialog Box*

The following options are available in the **Subzone Properties** dialog box:

General

Name

Type the required subzone name.

Description

Type the required subzone description.

Subzone definition rules

Add

Click to add a new subzone rule. The **Add Subzone Rule** dialog box displays. For more information, see Adding or Modifying Subzone Rules on page 173.

Edit

Double click the required subzone rule, or select the required subzone rule and click **Edit** to modify an existing subzone rule. The **Edit Subzone Rule** dialog box displays. For more information, see Adding or Modifying Subzone Rules on page 173.

Delete

Select the required subzone rule and click **Delete** to remove.

Maximum bandwidth per call within this subzone

Set the maximum bandwidth rate available per call for calls between endpoints within the same subzone. The default rate is 1024 Kbps.

Adding or Modifying Subzone Rules

To add a new subzone rule, click **Add** to display the **Add Subzone Rule** dialog box. To modify an existing subzone rule, double click the required subzone rule, or select the required subzone rule and click **Edit** to display the **Edit Subzone Rule** dialog box.

You can add or modify a subzone rule based on IP range or on IP subnet. IP range is the default option.

Warning Make sure there are no clashes between any IP range rule and any subnet IP rule. Clashes between rules may cause the LifeSize Gatekeeper to behave unpredictably.

IP Range Rules

The following options are available in the **Add Subzone Rule** and **Edit Subzone Rule** dialog box:

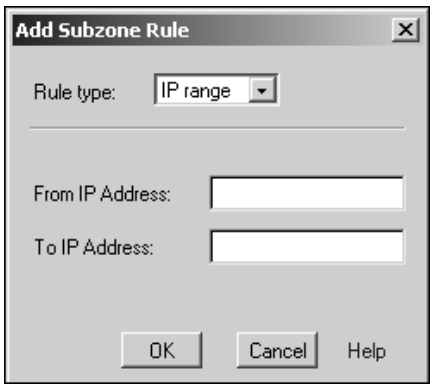

Figure 10-3 *Add Subzone Rule Dialog Box—IP Range*

Rule type

Displays **IP range** by default.

From IP Address

Type the lower limit of the range of IP addresses which will activate the rule.

To IP Address

Type the upper limit of the range of IP addresses which will activate the rule.

IP Subnet Rules

The following options are available in the **Add Subzone Rule** and **Edit Subzone Rule** dialog box:

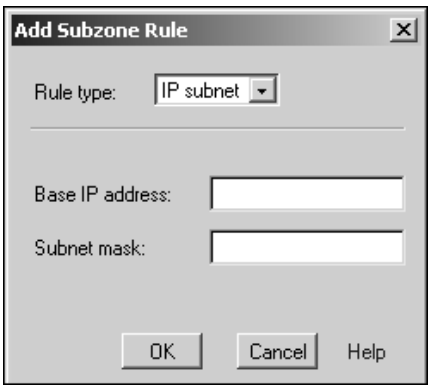

Figure 10-4 *Add Subzone Rule Dialog Box—IP Subnet*

Rule type

Select **IP subnet** from the drop-down list.

Base IP address

Type the base IP address that will activate the rule.

Subnet mask

Type the subnet mask that will activate the rule.

Bandwidth Policy

The **Bandwidth Policy** section of the **BW Policy** tab enables you to view and configure bandwidth policy settings which determine the bandwidths available between specific zones and subzones. For more information about subzones, see About Subzones on page 169.

Sample Topology with Subzones

Figure 10-5 on page 175 shows four Gatekeeper Zones (**A**, **B**, **C** and **D**), two subzones (**Aa** and **Ab**) and seven endpoints (**Aa1**, **Ab1**, **A1**, **B1**, **C1**, **D1** and **X**). Table 10-2 on page 176 defines the rules configured for this topology.

- Subzones **Aa** and **Ab** are in Zone A.
- Endpoint **Aa1** is in Subzone Aa.
- Endpoint **Ab1** is in Subzone Ab.
- Endpoint **A1** is in Zone A, but not in any subzone.
- Endpoints **B1**, **C1** and **D1** are in Zones B, C and D respectively.
- Endpoint **X** is not a member of any of the defined Gatekeeper Zones.

The arrows numbered 1 to 6 represent rules. For more information, see Subzone Rules on page 176.

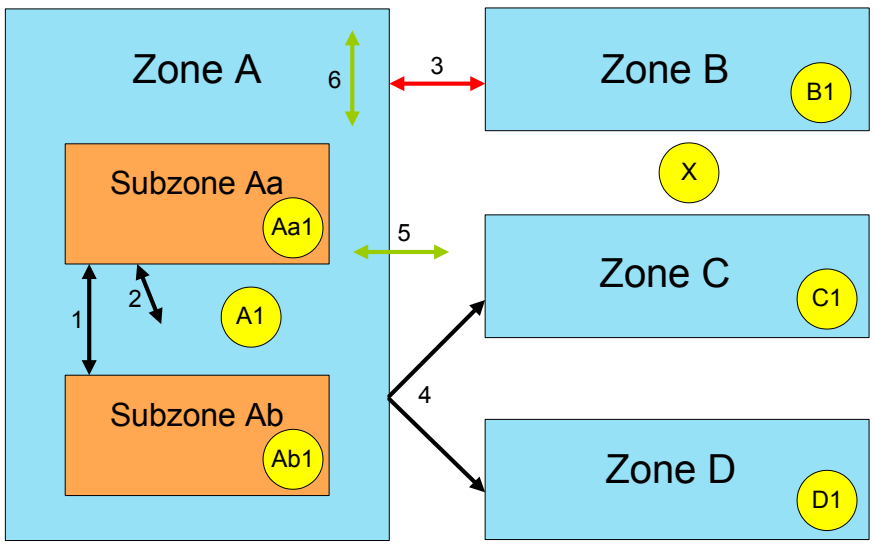

Figure 10-5 *Sample Subzone Topology*

SUBZONE RULES

This section describes the rules shown in Sample Subzone Topology on page 175.

SAMPLE RULES

Table 10-2 shows the available bandwidth according to the rules configured for a LifeSize Gatekeeper in Zone A of the sample topology in Figure 10-5.

Table 10-2 *Bandwidth Per Rule*

Rule number	For calls between ...	and between ...	Available bandwidth (Mbps)
1	Subzone Aa	Subzone Ab	5
2	Subzone Aa	Anywhere	10
3	Zone A	Zone B	20
4	Zone A	Zones C and D	20 (dedicated—see Dedicated Rules on page 178)
5	Zone A	Anywhere	25 (default—see Default Rules on page 180)
6	Any subzone	Anywhere	1 (default—see Default Rules on page 180)

Note Rule 6 is used for calls between endpoints in different subzones which are not governed by any other defined rule. For example, calls between endpoints A1 and Aa1 in Figure 10-5.

Table 10-3 shows which rules are activated by differing call scenarios.

Table 10-3 *Rules Used in Sample Call Scenarios*

Source endpoint	Destination endpoint	Rules used
Aa1	Ab1	Rules 1 and 2
Aa1	A1	Rule 2
Aa1	B1	Rules 2 and 3
Aa1	C1	Rules 2, 4 and 5
Aa1	D1	Rules 2, 4 and 5
Aa1	X	Rules 2 and 5
A1	B1	Rules 3 and 5
A1	C1	Rule 4
A1	X	Rule 5
Ab1	A1	Rule 6

APPLYING RULES

This section describes the order in which rules are applied to calls.

For inter-zone calls

1. All relevant dedicated rules are applied.
2. If there are no relevant dedicated rules, all relevant non-dedicated rules are applied.
3. If there are no relevant dedicated or non-dedicated rules, the default rule is applied.

For inter-subzone calls

1. All relevant dedicated rules are applied.
2. If there are no relevant dedicated rules, all relevant non-dedicated rules are applied.
3. Where no relevant subzone rule applies, the default rule will apply.

Note When both endpoints are in the same subzone, no rule will apply and the bandwidth limitation will be set via the **Subzone Properties** dialog box (Figure 10-2 on page 171).

Calculating Used Bandwidth

The bandwidth required by a call must be available via each of the rules used by that call. For example, the call between endpoints Aa1 and B1 in Table 10-3 uses rules 2 and 3. The bandwidth allowed by each of these rules is as follows, according to Table 10-2:

- Rule 2—10 Mbps
- Rule 3—20 Mbps

Assume that the call requires 5 Mbps of bandwidth and that no other calls are currently in progress. When the call connects, 5 Mbps will be used for each of Rules 2 and 3. The available bandwidth will fall to 5 Mbps for Rule 2, and to 15 Mbps for Rule 3.

Warning If you have not selected the **Reduce** option in the **Capacity** section of the **Settings** tab, a call will fail if there is not enough bandwidth available for any of the rules used by that call. The LifeSize Gatekeeper bandwidth restriction mechanism blocks the call on first rule that does not have enough bandwidth available.

Dedicated Rules

You can use dedicated rules with, for example, leased lines or for a dedicated network connection between subzones or zones. A dedicated rule (such as Rule 4 in Table 10-2) is a rule which applies to calls between specified endpoints, subzones or zones. For example, in Table 10-2, Rule 4 is a dedicated rule between Zone A and Zone C, and between Zone A and Zone D. A call governed by a dedicated rule will not be governed by any non-dedicated rule.

The bandwidth used for a call which activates a dedicated rule is not included in the used bandwidth calculation described in the Calculating Used Bandwidth section.

A non-dedicated rule can govern any call that is not dedicated.

Default Rules

A **default zone rule** (such as Rule 5 in Table 10-2) applies to any inter-zone call that does not match any of the defined inter-zone rules.

A **default subzone rule** (such as Rule 6 in Table 10-2) applies to any calls within the same zone that do not match any of the defined inter-subzone rules (dedicated or non-dedicated).

Configuring Bandwidth Policy

This section describes the configuration options in the **Bandwidth Policy** section of the **BW Policy** tab.

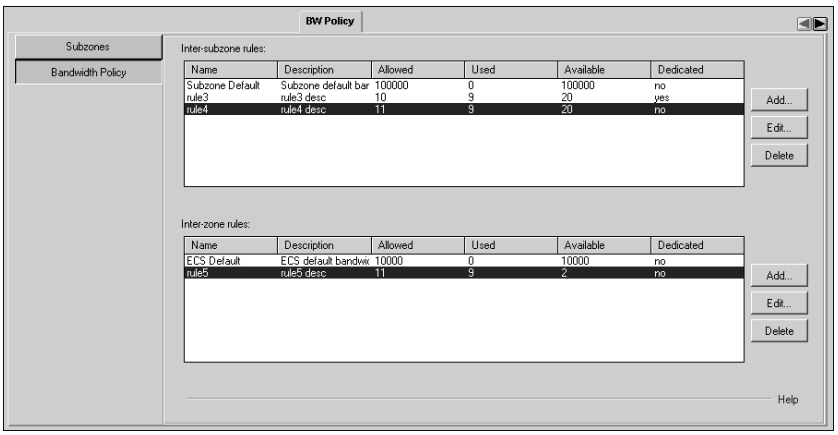

Figure 10-6 *BW Tab: Bandwidth Policy*

What You See

The following information is displayed in the **Bandwidth Policy** section of the **BW Policy** tab. Information is displayed for both inter-subzone rules and for inter-zone rules.

Table 10-4 *BW Tab: Bandwidth Policy Configuration*

Field	Description
Name	Displays the name of the specified rule.
Description	Displays the description of the specified rule.
Allowed	Displays the total bandwidth (in Kbps) allowed by the specified rule.

Table 10-4 BW Tab: Bandwidth Policy Configuration (continued)

Field	Description
Used	Displays the bandwidth (in Kbps) currently used by calls governed by the specified rule.
Available	Displays the free bandwidth (in Kbps) currently available to calls governed by the specified rule. **NOTE**: Displays 0 when available - used bandwidth < 0.
Dedicated	Indicates whether or not the rule applies to a specific dedicated connection only. For more information, see Dedicated Rules on page 178.

WHAT YOU CAN CONFIGURE

The following configuration options are available in the **Bandwidth Policy** section of the **BW Policy** tab:

INTER-SUBZONE RULES

Note Inter-subzone rules apply only to calls between endpoints located in the same LifeSize Gatekeeper zone.

Add

Click to add a new inter-subzone rule. The **Inter-subzone Bandwidth Rules** dialog box displays. For more information, see Adding or Modifying Inter-subzone Rules on page 182.

Edit

Double click the required inter-subzone rule, or select the required inter-subzone rule and click **Edit** to modify an existing inter-subzone rule. The **Inter-subzone Bandwidth Rules** dialog box displays. For more information, see Adding or Modifying Inter-subzone Rules on page 182.

Delete

Select the required inter-subzone rule and click **Delete** to remove.

INTER-ZONE RULES

Add

Click to add a new inter-zone rule. The **Inter-zone Bandwidth Rules** dialog box displays. For more information, see Adding or Modifying Inter-zone Rules on page 186.

Edit

Double click the required inter-zone rule, or select the required inter-zone rule and click **Edit** to modify an existing inter-zone rule. The **Inter-zone Bandwidth Rules** dialog box displays. For more information, see Adding or Modifying Inter-zone Rules on page 186.

Delete

Select the required inter-zone rule and click **Delete** to remove.

ADDING OR MODIFYING INTER-SUBZONE RULES

To create a new inter-subzone rule, click **Add** to display the **Inter-subzone Bandwidth Rules** dialog box. To modify an existing inter-subzone rule, double click the required inter-subzone rule, or select the required inter-subzone rule and click **Edit** to display the **Inter-subzone Bandwidth Rules** dialog box.

Note If you select the **Subzone Default** entry, the **Inter-subzone Bandwidth Rules** dialog box displays default settings only. For more information, see Viewing or Modifying the Default Inter-subzone Rule on page 185.

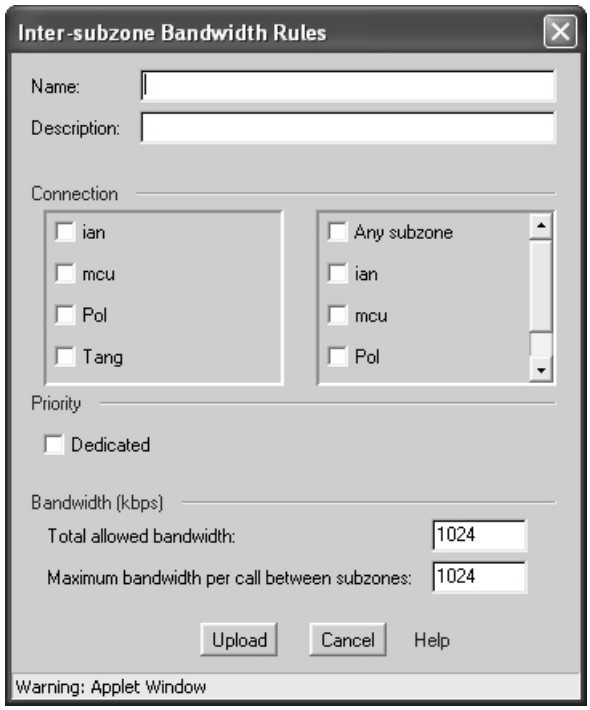

Figure 10-7 *Inter-subzone Bandwidth Rules Dialog Box*

The following options are available in the **Inter-subzone Bandwidth Rules** dialog box:

Name

Type the required name of the inter-subzone rule.

Description

Type the required description of the inter-subzone rule.

CONNECTION

You can apply the specified inter-subzone rules to the subzones displayed in the lists by checking the box next to the required subzones.

Check the **Any subzone** option to apply the specified inter-subzone rule to all calls within this zone.

PRIORITY

Dedicated

When checked, the call is not included in the used bandwidth calculation. A dedicated rule applies to a specific dedicated connection only. For more information, see Dedicated Rules on page 178.

BANDWIDTH (KBPS)

Total allowed bandwidth

Type the bandwidth (in Kbps) allowed by the specified inter-subzone rule.

Maximum bandwidth per call between subzones

Define the maximum bandwidth available per call for calls between endpoints in different subzones. The default bandwidth rate is 1024 Kbps.

When an endpoint is registered to the LifeSize Gatekeeper but not included in any subzone, a rule defined between a subzone X and any subzone will apply to a call between that endpoint and subzone X.

A subzone rule defined between a subzone X and any subzone will not apply to calls between two endpoints which are both located within subzone X.

Note The **Any subzone** option does not refer to out-of-zone calls.

VIEWING OR MODIFYING THE DEFAULT INTER-SUBZONE RULE

The default inter-subzone rule applies to any intra-zone call that does not match any of the configured inter-subzone bandwidth rules.

Double click the **Subzone Default** inter-subzone rule, or select the **Subzone Default** inter-subzone rule and click **Edit**. The **Inter-subzone Bandwidth Rules** dialog box displays indicating default settings.

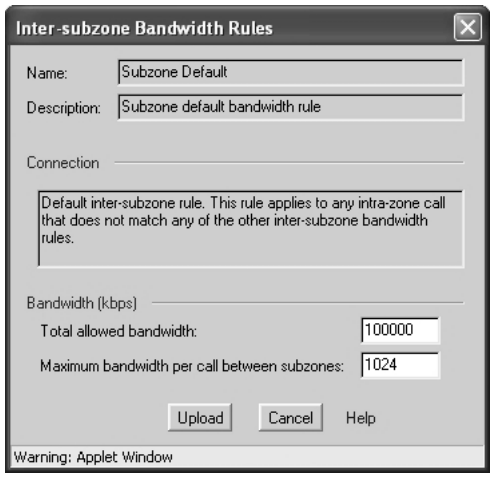

Figure 10-8 *Inter-subzone Bandwidth Rules Dialog Box—Default*

The following information is displayed in the default **Inter-subzone Bandwidth Rules** dialog box:

Name

Displays the name of the default inter-subzone rule.

Description

Displays the description of the default inter-subzone rule.

BANDWIDTH (KBPS)

Total allowed bandwidth

Type the bandwidth (in Kbps) allowed by the default inter-subzone rule.

Maximum bandwidth per call between subzones

Define the maximum bandwidth available per call for calls between endpoints in different subzones. The default bandwidth rate is 1024 Kbps.

When an endpoint is registered to the LifeSize Gatekeeper but not included in any subzone, a rule defined between a subzone X and any subzone will apply to a call between that endpoint and subzone X.

A subzone rule defined between a subzone X and any subzone will not apply to calls between two endpoints which are both located within subzone X.

Note The **Any subzone** option does not refer to out-of-zone calls.

Adding or Modifying Inter-zone Rules

To create a new inter-zone rule, click **Add** to display the **Inter-zone Bandwidth Rules** dialog box. To modify an existing inter-zone rule, double click the required inter-zone rule, or select the required inter-zone rule and click **Edit** to display the **Inter-zone Bandwidth Rules** dialog box.

Note If you select the LifeSize Gatekeeper **Default** entry, the **Inter-zone Bandwidth Rules** dialog box displays default settings only. For more information, see Viewing or Modifying the Default Inter-subzone Rule on page 185.

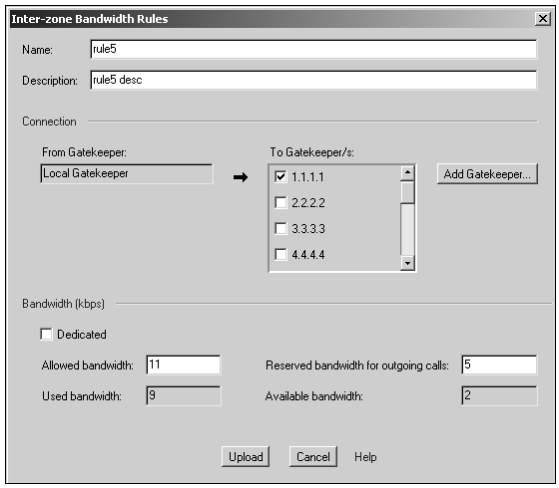

Figure 10-9 *Inter-zone Bandwidth Rules Dialog Box*

The following options are available in the **Inter-zone Bandwidth Rules** dialog box:

Name

Type the required name of the inter-zone rule.

Description

Type the required description of the inter-zone rule.

CONNECTION

From Gatekeeper

Displays **Local Gatekeeper**. Read only.

To Gatekeeper/s

Select the required destination gatekeepers from the list displayed.

Add Gatekeeper

Click to add additional gatekeepers. For more information, see Adding a Gatekeeper on page 188.

BANDWIDTH (KBPS)

Dedicated

When checked, the call is not included in the used bandwidth calculation.

Allowed bandwidth

Type the bandwidth (in Kbps) allowed by the specified inter-zone rule.

Reserved bandwidth for outgoing calls

Type the bandwidth (in Kbps) that you wish you to reserve for outgoing calls only. Reserved bandwidth is deducted from the total allowed bandwidth.

Used bandwidth

Displays the bandwidth (in Kbps) currently used by calls governed by the specified inter-zone rule.

Available bandwidth

Displays the free bandwidth (in Kbps) currently available to calls governed by the specified inter-subzone rule.

ADDING A GATEKEEPER

Click **Add Gatekeeper** to display the **Add Gatekeeper** dialog box for adding additional gatekeepers to the displayed list.

Type the IP address of the gatekeeper you wish to add.

VIEWING OR MODIFYING THE DEFAULT INTER-ZONE RULE

The default inter-zone rule applies to any inter-zone call that does not match any of the configured inter-zone bandwidth rules.

Double click the LifeSize Gatekeeper **Default** inter-zone rule, or select the LifeSize Gatekeeper **Default** inter-zone rule and click **Edit**. The **Inter-zone Bandwidth Rules** dialog box displays indicating default settings.

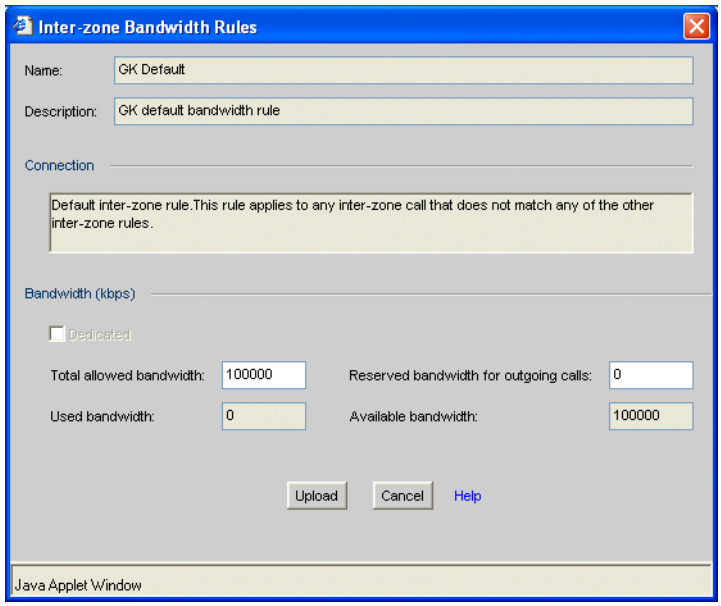

Figure 10-10 *Inter-zone Bandwidth Rules Dialog Box—Default*

The following information is displayed in the default **Inter-zone Bandwidth Rules** dialog box:

Name

Displays the name of the default inter-zone rule.

Description

Displays the description of the default inter-zone rule.

BANDWIDTH (KBPS)

Dedicated

A default rule cannot be dedicated. Disabled for the default inter-zone rule.

Allowed bandwidth

Type the bandwidth (in Kbps) allowed by the default inter-zone rule.

Reserved bandwidth for outgoing calls

Type the bandwidth (in Kbps) that you wish you to reserve for outgoing calls only.

Used bandwidth

Displays the bandwidth (in Kbps) currently used by calls governed by the default inter-zone rule.

Available bandwidth

Displays the bandwidth (in Kbps) currently available to calls governed by the default inter-zone rule.

11

CALL CONTROL TAB

ABOUT THE CALL CONTROL TAB

The **Call Control** tab enables you to monitor current calls. You can view additional details about a specific call including general information, details about the source of the call and details about the destination of the call. You can also disconnect one or all of the calls.

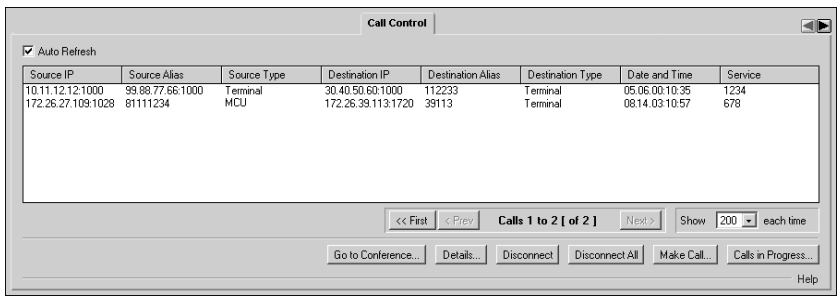

Figure 11-1 *Call Control Tab*

What You See

The following information is displayed in the **Call Control** tab:

Auto Refresh

When checked, the LifeSize Gatekeeper checks whether or not the information in the **Call Control** tab has changed at predetermined intervals of ten seconds. Any changes are updated automatically to the **Call Control** tab.

Table 11-1 *Call Control Tab Details*

Field	Description
Source IP	Displays the IP address of the source of the call.
Source Alias	Displays the first of the source endpoint aliases.
Source Type	Displays the source endpoint type.
Destination IP	Displays the IP address of the destination of the call.
Destination Alias	Displays the first of the destination endpoint aliases.
Destination Type	Displays the destination endpoint type.
Date and Time	Displays the date and time the call began in the following format: mm/dd/yy_hh:mm_AM/PM.
Service	Indicates whether or not the call is to a service, and if so, to which service.

Status Bar

The status bar below the list of calls indicates which block of calls is displayed in the **Call Control** tab, and the total number of calls in the LifeSize Gatekeeper. For example, **Calls 1 to 50 [of 110]** indicates that the first block of 50 calls is displayed out of 110 calls in the LifeSize Gatekeeper. When there are no calls, **No calls** is displayed.

What You Can Configure

The following buttons are available for displaying and performing actions on the calls:

First

Click the **First** button to display the first block of calls.

Previous

Click the **Previous** button to display the previous block of calls.

Next

Click the **Next** button to display the next block of calls.

Show *number of calls* each time

Select the number of calls you want to be displayed as a block of calls. You can display blocks of 10-200 calls in increments of 10.

Go to Conference

Select an LifeSize Multipoint conference and click to display the LifeSize Multipoint **Conference Control** interface.

Details

Click the **Details** button to view the call details in the **Call Details** window. For more information, see Viewing Call Details on page 194.

Disconnect

Select a call and click the **Disconnect** button to disconnect the selected call. The call is disconnected but the endpoint remains in the registration database.

Disconnect All

Click the **Disconnect All** button to disconnect all the current calls in the **Call Control** tab.

Make Call

Click the **Make Call** button to open the **Make Call** dialog box for third party control over calls between two endpoints. For more information about Third Party Call Control, see Enabling Third Party Call Control on page 197 and Third Party Call Control on page 14.

Note The **Make Call** dialog box displays only when the LifeSize Gatekeeper is configured to operate in **Call Setup (Q.931) and Call Control (H.245)** mode in the **Routing mode** field in the **Calls** section of the **Settings** tab.

Calls in Progress

Click the **Calls in Progress** button to view the call details of all third party-controlled calls currently in progress in the **Calls in Progress** window. For more information, see Viewing Third Party Call Control Details on page 204.

VIEWING CALL DETAILS

The **Call Details** window enables you to view the call details and displays general call information, source information and destination information.

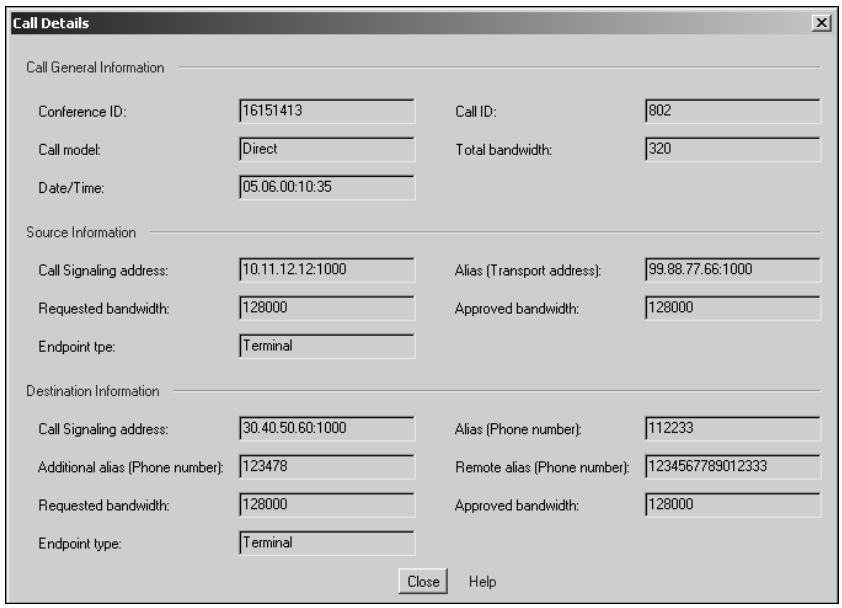

Figure 11-2 *Call Details Dialog Box*

Click the call for which you want to view the call details in the **Call Control** tab and then click the **Details** button to open the **Call Details** dialog box. The following information is displayed:

CALL GENERAL INFORMATION

Conference ID

Displays the unique ID that identifies the call.

Call ID

Displays the unique value created by the calling endpoint and passed in various H.225.0 messages. The **Call ID** associates RAS messages with Q.931 messages in the same call.

Call model

Indicates whether the call is Routed or Direct. A call in Routed Mode routes the Call Setup channel (Q.931) and sometimes the Control channel (H.245) via the LifeSize Gatekeeper. A call in Direct Mode routes the Call Setup (Q.931) and Control (H.245) channels to form a direct connection between two endpoints without LifeSize Gatekeeper intervention. A call in Call Setup (Q.931) and Call Control (H.245) Routed Mode routes the Call Setup channel and the Control channel via the LifeSize Gatekeeper.

Total bandwidth

Displays the total amount of bandwidth (in Kbps) used by the call.

Date/Time

Displays the date and time the call began.

Source Information

Call Signaling address

Displays the IP address and port of the calling endpoint.

Alias

Displays the alias of the calling endpoint. The text in parentheses after **Alias** changes according to the type of alias.

Requested bandwidth

Displays the bandwidth (in Kbps) requested by the calling endpoint for this call.

Approved bandwidth

Displays the bandwidth (in Kbps) the LifeSize Gatekeeper made available to the calling endpoint.

Endpoint type

Displays the source endpoint type.

Destination Information

Call Signaling address

Displays the IP address and port of the called endpoint.

Alias

Displays the alias of the destination endpoint. The text in parentheses after **Alias** changes according to the type of alias.

Additional alias

Displays the additional alias number for a call with more than one B channel. The text in parentheses after **Additional alias** changes according to the type of alias.

Remote alias

Displays the alias number of the called endpoint on the remote IP network in calls between multiple gateways. The text in parentheses after **Remote alias** changes according to the type of alias.

Requested bandwidth

Displays the bandwidth (in Kbps) requested by the called endpoint for the call.

Approved bandwidth

Displays the bandwidth (in Kbps) the LifeSize Gatekeeper made available to the called endpoint for the call.

Endpoint type

Displays the destination endpoint type.

Enabling Third Party Call Control

The **Make Call** dialog box allows you to initiate calls through the LifeSize Gatekeeper. The **Make Call** dialog box displays details of calls initiated using this option.

To enable Third Party Call Control, the LifeSize Gatekeeper must be configured to operate in **Call Setup (Q.931) and Call Control (H.245)** mode in the **Routing mode** field in the **Calls** section of the **Settings** tab.

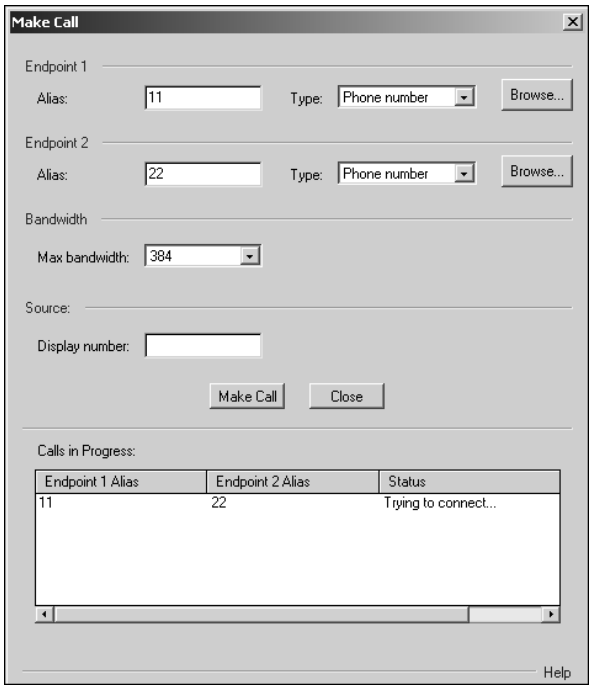

Figure 11-3 *Make Call Dialog Box*

The following options are available in the **Make Call** dialog box:

Endpoint 1

Alias

Type the alias of the source endpoint of the call or click **Browse** to select an alias from the list of endpoints registered to the LifeSize Gatekeeper.

Type

Select the alias type of the source endpoint of the call from the drop-down list or click **Browse** to select an alias type.

Browse

Click **Browse** to open the **Select Endpoint** dialog box for selecting an alias and alias type for the source endpoint of a third party-controlled call. For more information, see Specifying Third Party Control Call Aliases on page 200.

ENDPOINT 2

Alias

Type the alias of the destination endpoint of the call or click **Browse** to select an alias.

Type

Select the alias type of the destination endpoint of the call from the drop-down list or click **Browse** to select an alias type.

Browse

Click **Browse** to open the **Select Endpoint** dialog box for selecting an alias and alias type for the destination endpoint of a third party-controlled call. For more information, see Specifying Third Party Control Call Aliases on page 200.

BANDWIDTH

Max bandwidth

Select the maximum bandwidth from the drop-down list for the third party-controlled call.

SOURCE

Display number

Displays the Calling Party Number that the LifeSize Gatekeeper sends to endpoints participating in the call.

Make Call

Click to initiate a third party-controlled call between the endpoints specified in the **Make Call** dialog box. For more information, see Viewing Third Party Call Control Details on page 204.

Note Successfully established calls appear in the **Call Control** tab table.

Close

Click to close the **Make Call** dialog box and to return to the **Call Control** tab.

Calls in Progress

Endpoint 1 Alias

Displays the alias of the source endpoint in a third party-controlled call currently in progress.

Endpoint 2 Alias

Displays the alias of the destination endpoint in a third party-controlled call currently in progress.

Status

Displays the status of a third party-controlled call currently in progress. Options are **OK** (when the call has successfully connected and is in progress), **Trying to connect ...** and **Failed**.

Specifying Third Party Control Call Aliases

The **Select Endpoint** dialog box enables you to see endpoints that are predefined and online (registered). You can specify the alias and the alias type for the source and destination endpoints in a third party-controlled call, and for a gateway or an LifeSize Multipoint.

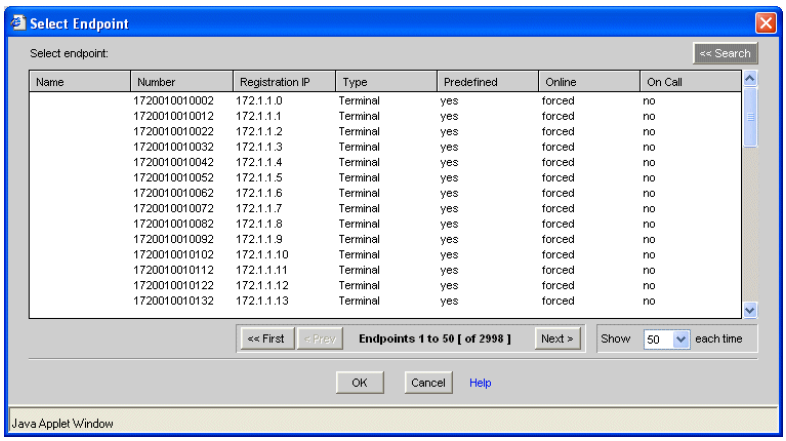

Figure 11-4 *Select Endpoint Dialog Box*

The following information is displayed in the **Select Endpoint** dialog box:

Table 11-2 *Select Endpoint Configuration*

Field	Description
Name	Displays the H.323 alias name of the endpoint. Where an endpoint has more than one alias, only the first one is displayed.
Number	Displays the E.164 alias number of the endpoint. Where an endpoint has more than one alias, only the first one is displayed.
Registration IP	Displays the IP address of the endpoint.
Type	Displays the type of endpoint—terminal, MCU or gateway.
Predefined	Indicates whether or not the endpoint has been predefined.
Online	Indicates whether or not the endpoint is registered.
On Call	Indicates whether or not the endpoint is participating in the current LifeSize Gatekeeper session.

STATUS BAR

Upon completing the search for an endpoint, the status bar below the list of endpoints displays **Search completed**. Otherwise, the status bar indicates which block of endpoints is displayed in the **Endpoints** section of the **Endpoints** tab, and the total number of endpoints in the LifeSize Gatekeeper database. For example, **Endpoints 1 to 20 [of 101]** indicates that the first block of 20 endpoints is displayed out of 101 endpoints in the LifeSize Gatekeeper database. When there are no endpoints registered in the LifeSize Gatekeeper database **No endpoints registered** is displayed.

The following buttons are available for searching for, displaying and configuring LifeSize Gatekeeper endpoints:

Search/Close Search

Click **Search** or **Close Search** to open or close the search engine. When you close the search engine, the endpoints are displayed from the beginning of the list.

Look for endpoints where the ... is ...

Select the filter through which you want to perform the search from the drop-down list: **phone number**, **name**, **URL address**, **transport address** or **e-mail address**. Type the details of one of the above options for which you are searching. You must type the *full* alias.

Note The alias is case-sensitive.

Find

Click the **Find** button to perform the search.

First

Click the **First** button to display the first block of endpoints.

Previous

Click the **Previous** button to display the previous block of endpoints.

Next

Click the **Next** button to display the next block of endpoints.

Show *number of endpoints* each time

Select the number of endpoints you want to be displayed as a block of endpoints. You can display blocks of 10-200 calls in increments of 10.

To specify the alias and alias type for a source (or destination) endpoint in third party-controlled calls

1. Click **Browse** in the **Source** (or **Destination**) group box in the **Make Call** dialog box.

   The **Select Endpoint** dialog box displays.
2. Double click an entry in the **Select Endpoint** table of type **Terminal**, or select an entry in the **Select Endpoint** table of type **Terminal** and click **OK**.

   The **Make Call** dialog box displays. The values in the **Name** and **Type** columns of the **Select Endpoint** table for the specified endpoint appear in the **Alias** and **Alias Type** fields of the **Source** (or **Destination**) group box in the **Make Call** dialog box.

To specify the alias for a source (or destination) gateway in third party-controlled calls

1. Click **Browse** in the **Source** (or **Destination**) group box in the **Make Call** dialog box.

   The **Select Endpoint** dialog box displays.
2. Double click an entry in the **Select Endpoint** table of type **Gateway**, or select an entry in the **Select Endpoint** table of type **Gateway** and click **OK**.

   The **Gateway Info** dialog box displays (Figure 11-5).
3. Select the required service from the drop-down list of supported gateway services and service descriptions, and type a dialing number.

   The alias is generated by placing the selected service number before the specified dialing number. For example, if the selected service number is **86** and the specified dialing number is **45**, the alias created is **8645**.

4 Click **OK**.

The generated alias appears in the **Alias** field of the **Source** (or **Destination**) group box. **Gateway** appears in the **Alias Type** field.

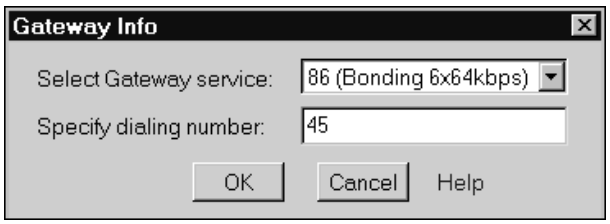

Figure 11-5 *Gateway Info Dialog Box*

To specify the alias for a source (or destination) LifeSize Multipoint in third party-controlled calls

1 Click **Browse** in the **Source** (or **Destination**) group box in the **Make Call** dialog box.

The **Select Endpoint** dialog box displays.

2 Double click an entry in the **Select Endpoint** table of type **MCU**, or select an entry in the **Select Endpoint** table of type **MCU** and click **OK**.

The **MCU Info** dialog box displays (Figure 11-6).

3 Select the required service from the drop-down list of supported LifeSize Multipoint services and service descriptions, and type a conference extension number.

The alias is generated by placing the selected service number with the specified conference extension number. For example, if the selected service number is **77** and the specified conference extension number is **123**, the alias created is **77123**.

4 Click **OK**.

The generated alias appears in the **Alias** field of the **Source** (or **Destination**) group box. **MCU** appears in the **Alias Type** field.

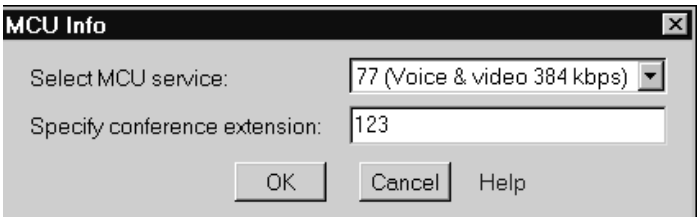

Figure 11-6 *MCU Info Dialog Box*

VIEWING THIRD PARTY CALL CONTROL DETAILS

The **Calls in Progress** window enables you to view the call details of all third party-controlled calls currently in progress, and displays source and destination information.

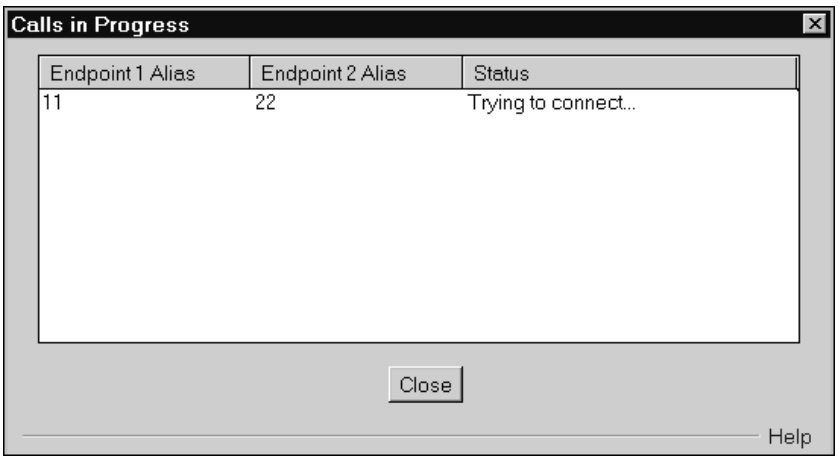

Figure 11-7 *Calls in Progress Window*

The following information is displayed in the **Calls in Progress** window:

Table 11-3 *Calls in Progress Configuration*

Field	Description
Endpoint 1 Alias	Displays the alias of the source endpoint in a third party-controlled call currently in progress.
Endpoint 2 Alias	Displays the alias of the destination endpoint in a third party-controlled call currently in progress.
Status	Displays the status of a third party-controlled call currently in progress. Options are **OK** (when the call has successfully connected and is in progress), **Trying to connect ...** and **Failed**.

12

FORWARD & FALLBACK TAB

ABOUT THE FORWARD & FALLBACK TAB

The **Forward & Fallback** tab enables you to view and configure Call Forwarding and Call Fallback rules. You can define different Forwarding and Fallback rules for an endpoint via the following sections:

- Forwarding
- Fallback

For information on Call Forwarding, see About Call Forwarding.

For information on Call Fallback, see About Call Fallback on page 208.

ABOUT CALL FORWARDING

A Forwarding service occurs when endpoint B calls endpoint A and the LifeSize Gatekeeper redirects the call to endpoint C. The LifeSize Gatekeeper supports three types of Call Forwarding:

- **Unconditional** enables an administrator to define an endpoint to have all its calls redirected to another endpoint. The LifeSize Gatekeeper forwards all calls without applying any conditions.
- **On Busy** enables an administrator to define an endpoint to have its calls redirected to another endpoint when it is busy. The LifeSize Gatekeeper forwards calls when the endpoint is busy.
- **On No Answer** enables an administrator to define an endpoint to have its calls redirected to another endpoint when there is no reply. The LifeSize Gatekeeper forwards calls when there is no reply from the endpoint.

Call Forwarding creates a full call between the *activating* endpoint and the *diverted-to* endpoint. Call Forwarding On Busy and Call Forwarding On No Answer attempt to create a call to the original destination endpoint. If the attempt fails because the endpoint is busy or there is no reply, the same call is executed to the diverted-to endpoint.

Note An activating endpoint does not need to be registered with the LifeSize Gatekeeper. Whether an activating endpoint is registered with the LifeSize Gatekeeper or not, the LifeSize Gatekeeper searches for Forwarding rules for this endpoint. If such Forwarding rules exist, the LifeSize Gatekeeper forwards the call to the diverted-to destination.

About Call Fallback

The LifeSize Gatekeeper supports Call Fallback in the following cases:

- **On Not Located**—The LifeSize Gatekeeper cannot resolve a destination address in the IP network.
- **On BW capacity limit**—The LifeSize Gatekeeper reaches the maximum bandwidth rate setting for any one of the configured endpoints, groups, subzones or zones.
- **Other**—A call is unsuccessful for any reason other than those already defined. For example, internal LifeSize Gatekeeper failure, an invalid service or an invalid exit zone prefix.

You can configure the LifeSize Gatekeeper to behave in one of the following ways:

- Route the call to an alias.
- Route the call to a service prefix.
- Route the call to the ISDN network via a gateway.
- Reject the call.

Forwarding

The **Forwarding** section of the **Forward & Fallback** tab enables you to define sets of Forwarding rules for each endpoint listed, and to add and modify rules and endpoints.

Note Call Forwarding does not function with the Third Party Call Control feature.

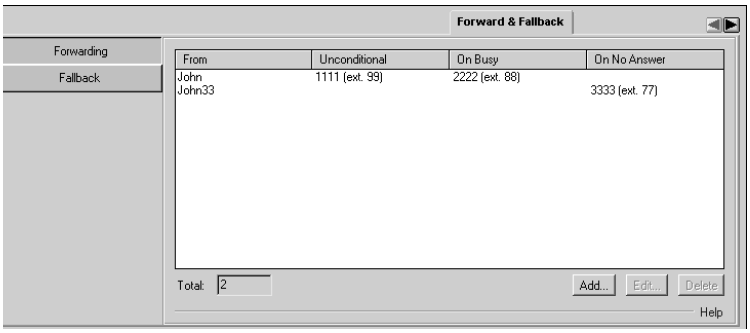

Figure 12-1 *Forward & Fallback Tab: Forwarding*

WHAT YOU SEE

The following information is displayed in the **Forwarding** section of the **Forward & Fallback** tab:

Table 12-1 *Forward & Fallback Tab: Forwarding Configuration*

Field	Description
From	Displays the alias or IP address of the activating endpoint.
Unconditional	Displays the alias or IP address to which calls are unconditionally forwarded (the diverted-to address). **Unconditional** indicates that the activating endpoint will have all its calls redirected to another endpoint. The administrator configures the LifeSize Gatekeeper to forward all calls without applying any conditions regarding the state of the activating endpoint. The activating endpoint can be offline at any point.
On Busy	Displays the alias (and extension) or IP address to which calls are forwarded (the diverted-to address) when the activating endpoint is busy. **On Busy** indicates that the activating endpoint will have its calls redirected to another endpoint when it is busy. The administrator configures the LifeSize Gatekeeper to forward calls when the activating endpoint is busy.

Table 12-1 Forward & Fallback Tab: Forwarding Configuration (continued)

Field	Description
On No Answer	Displays the alias (and extension) or IP address to which calls are forwarded (the diverted-to address) when there is no answer from the activating endpoint. **On No Answer** indicates that the activating endpoint will have its calls redirected to another endpoint when there is no response. The administrator configures the LifeSize Gatekeeper to forward calls when there is no response from the activating endpoint.

Total

Indicates the total number of standard Call Forwarding rules currently in the LifeSize Gatekeeper database.

What You Can Configure

The following options are available for configuring Call Forwarding:

Add

Click to add a Call Forwarding rule to the LifeSize Gatekeeper database. For more information, see Adding or Modifying a Call Forwarding Rule on page 211.

Edit

Double click the relevant entry in the list, or select the relevant entry and click **Edit** to modify the selected Call Forwarding rule. For more information, see Adding or Modifying a Call Forwarding Rule on page 211.

Delete

Click the **Delete** button to delete the selected Call Forwarding rule from the LifeSize Gatekeeper database.

Adding or Modifying a Call Forwarding Rule

To add a Call Forwarding rule to the LifeSize Gatekeeper database, click **Add** to display the **Add Forward** dialog box. To modify an existing Call Forwarding rule in the LifeSize Gatekeeper database, double click the required rule, or select the required rule and click **Edit** to display the **Edit Forward** dialog box.

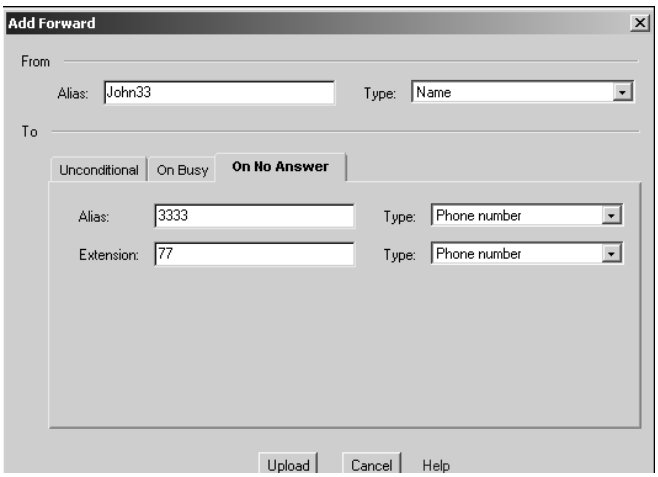

Figure 12-2 *Add Forward Dialog Box*

The following options are available in the **Add Forward** and **Edit Forward** dialog box:

From

Alias

Enter or modify the alias of the forwarding endpoint. You can use up to 255 characters.

Type

Select the type of alias: **Phone number**, **Name**, **URL address**, **Transport address** (in the "IP address: port number" format), **E-mail address** or **Party number**. If you select **Party number**, the **Number Type** field is displayed. For more information on Party number, see the **Endpoints** chapter.

To

Unconditional

Select this tab to define a rule for Unconditional Forwarding.

Note When Unconditional Forwarding is enabled, the Unconditional Forwarding rule overrides both the Forwarding On Busy rule and the Forwarding On No Answer rule.

On Busy

Select this tab to define a rule for Forward On Busy.

On No Answer

Select this tab to define a rule for Forward On No Answer.

Note Call Forwarding **On Busy** and **On No Answer** is not available when the **Direct** option is selected in the **Routing mode** field in the **Calls** section of the **Settings** tab.

Alias

Enter or modify the alias of the endpoint to which the calls are forwarded. You can use up to 255 characters.

Type

Select the type of alias to which the calls are forwarded (as listed at Type on page 211).

Extension

Enter or modify the extension of the endpoint to which the calls are forwarded. This option is for calls which pass through multiple gateways.

Type

Select the type of alias to which the calls are forwarded (as listed at Type on page 211).

Upload

Click the **Upload** button to add the Call Forwarding service rule set to the LifeSize Gatekeeper database.

FALLBACK

The **Fallback** section of the **Forward & Fallback** tab enables you to configure rules to deal with cases where:

- The LifeSize Gatekeeper cannot resolve a destination address in the IP network.
- The LifeSize Gatekeeper reaches the maximum bandwidth rate setting for any one of the configured endpoints, groups, subzones or zones.
- The LifeSize Gatekeeper receives an LRJ message from a Neighbor Gatekeeper because a destination endpoint cannot be located.
- The LifeSize Gatekeeper times out before receiving an LRJ message from Neighbor Gatekeeper because the timeout interval for an LRQ message has passed (for example, due to network failure).
- Resolution of a destination address fails for any other reason (for example, a call is to a disallowed service).

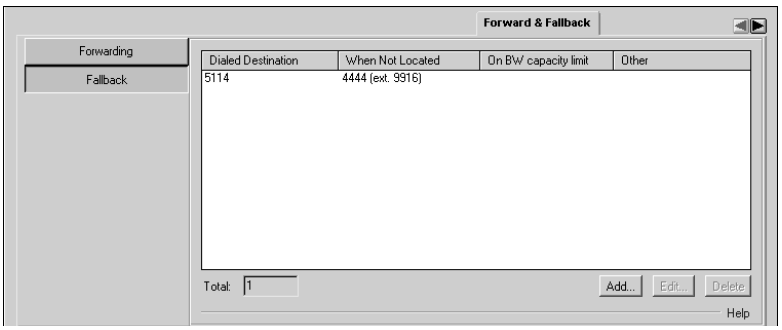

Figure 12-3 *Forward & Fallback Tab: Fallback*

What You See

The following information is displayed in the **Fallback** section of the **Forward & Fallback** tab:

Figure 12-4 *Forward & Fallback Tab: Fallback Configuration*

Field	Description
Dialed Destination	Indicates the number dialed destination number.
When Not Located	Indicates the destination to which the call is forwarded by the defined rule when the LifeSize Gatekeeper fails to locate the dialed destination on the IP network.
On BW capacity limit	Indicates the destination to which the call is forwarded by the defined rule when Call Setup to the dialed destination endpoint is unsuccessful because the LifeSize Gatekeeper has reached the maximum bandwidth rate setting for any one of the configured endpoints, groups, subzones or zones.
Other	Indicates the destination to which the call is forwarded by the defined rule when call is unsuccessful for any reason other than those already defined. For example, internal LifeSize Gatekeeper failure, an invalid service or an invalid exit zone prefix.

Total

Indicates the total number of standard Call Fallback rules currently in the LifeSize Gatekeeper database.

What You Can Configure

The following options are available for configuring Call Fallback:

Add

Click to add a Call Fallback rule to the LifeSize Gatekeeper database. For more information, see Adding or Modifying a Call Fallback Rule on page 215.

Edit

Double click the relevant entry in the list, or select the relevant entry and click **Edit** to modify the selected Call Fallback rule. For more information, see Adding or Modifying a Call Fallback Rule on page 215.

Delete

Click the **Delete** button to delete the selected Call Fallback rule from the LifeSize Gatekeeper database.

Adding or Modifying a Call Fallback Rule

To add a new Call Fallback rule, click **Add** to display the **Add Fallback** dialog box. To modify an existing Call Fallback rule in the LifeSize Gatekeeper database, double click the required rule, or select the required rule and click **Edit** to display the **Edit Fallback** dialog box.

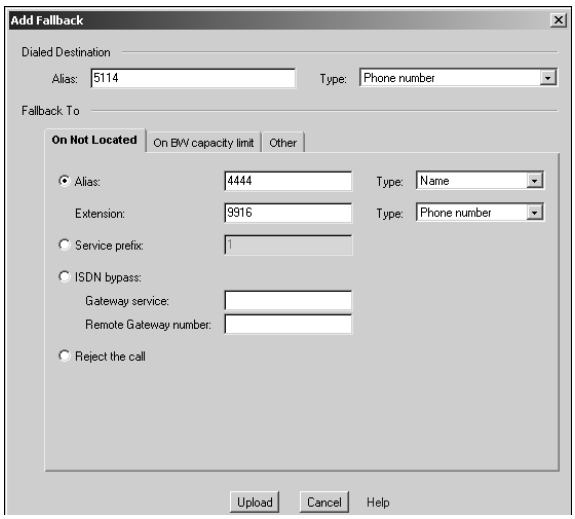

Figure 12-5 *Add Fallback Dialog Box*

The following options are available in the **Add Fallback** and **Edit Fallback** dialog box:

Dialed Destination

Alias

Enter or modify the alias of the forwarding endpoint. You can use up to 255 characters.

Type

Select the type of alias: **Phone number**, **Name**, **URL address**, **Transport address** (in the "IP address: port number" format), **E-mail address** or **Party number**. If you select **Party number**, the **Number Type** field is displayed. For more information on Party number, see the **Endpoints** chapter.

FALLBACK TO

The **Fallback To** section enables you to configure a Call Fallback policy in cases where the LifeSize Gatekeeper fails to locate the dialed destination on the IP network (using the **On Not Located** tab), in cases where Call Setup to the dialed destination endpoint is unsuccessful due to network failure (using the **On BW capacity limit** tab), and in cases where a call is unsuccessful for any other reason, such as internal LifeSize Gatekeeper failure, an invalid service or an invalid exit zone prefix (using the **Other** tab).

Each tab enables you to select to where the LifeSize Gatekeeper Call Fallback policy sends a call. The available options are

- To an alias.
- To a service prefix.
- To the ISDN network via a gateway.
- Reject the call.

Note Call Fallback **On BW capacity limit** is not available when the **Direct** option is selected in the **Routing mode** field in the **Calls** section of the **Settings** tab.

On Not Located

Select this tab to define a Call Fallback rule for when the LifeSize Gatekeeper fails to locate the dialed destination on the IP network because

- The destination endpoint cannot be located.
- The timeout interval for an LRQ message has passed (for example, due to network failure).

On BW capacity limit

Select this tab to define a Call Fallback rule for when Call Setup to the dialed destination endpoint is unsuccessful because the LifeSize Gatekeeper has reached the maximum bandwidth rate setting for any one of the configured endpoints, groups, subzones or zones.

Alias

Select to route calls to a specified alternate H.323 alias address (such as an Interactive Voice Response). Type the alias of the H.323 endpoint to which the calls are forwarded. You can use up to 255 characters.

Type

Select the type of alias to which the calls are forwarded (as listed at Type on page 211).

Extension

Type the extension of the endpoint to which the calls are forwarded. This option is for calls which pass through multiple gateways.

Type

Select the type of alias to which the calls are forwarded (as listed at Type on page 211).

Service prefix

Select to send calls through the local gateway or to use another service. Type the prefix of the required service. The LifeSize Gatekeeper adds the service prefix to the number and dial number of the destination endpoint.

Note To send calls via the gateway, type the service prefix of the required gateway and ensure that the destination endpoint alias is an E.164 alias.

ISDN bypass

Check to forward calls over the ISDN network via a gateway.

When there is not enough bandwidth over the IP network to carry further calls, the LifeSize Gatekeeper can send a call through the local gateway for transmission over the ISDN network. To enable ISDN bypass, you must configure the service prefix and the number of the gateway through which you want to route calls.

Reject the call

Select to reject a call when the LifeSize Gatekeeper cannot find a location address.

13

HIERARCHY TAB

ABOUT THE HIERARCHICAL GATEKEEPER STRUCTURE

A hierarchical LifeSize Gatekeeper structure can support version 2 of the LifeSize Gatekeeper Dial Plan. A hierarchical structure enables each LifeSize Gatekeeper to serve many dialing zones and to strip and attach dialing prefixes. The hierarchy allows each zone to support more than 50 calls and 250 registrations. You can configure the LifeSize Gatekeeper to support the required version of the LifeSize Gatekeeper Dial Plan in the **Basics** section of the **Settings** tab. For more information about the LifeSize Gatekeeper Dial Plan, see Dial Plan on page 57 and the LifeSize Gatekeeper Dial Plan version 2 appendix.

About the Hierarchy Tab

The **Hierarchy** tab enables you to create a hierarchy of gatekeepers by adding a parent, neighbors and children to the LifeSize Gatekeeper. You can configure a list of parent filters and choose whether or not to route calls to unresolved zones via the Cisco Proxy. You specify these parameters in the following sections of the **Hierarchy** tab, which are described in detail below:

- Parent Gatekeeper
- Neighbors
- Children

Note Setting the **Dial Plan** field in the **Basics** section of the **Settings** tab to **Version 2** replaces the **Neighbors** tab with the **Hierarchy** tab and opens the **Services** and **Global Services** sections of the **Services** tab. For more information about the **Neighbors** tab, see the Neighbors Tab chapter.

Note When the **Use Central Database** option is checked in the **Central Database** section of the **Settings** tab and **Version 2** is selected in the **Dial Plan version** field in the **Basics** section of the **Settings** tab, the information displayed in the **Hierarchy** tab is read-only. For more information about the Central Database, see Central Database on page 87. For more information about the Dial Plan, see Dial Plan on page 57 and the LifeSize Gatekeeper Dial Plan version 2 appendix.

Parent Gatekeeper

The **Parent Gatekeeper** section of the **Hierarchy** tab enables you to configure a Parent Gatekeeper for the LifeSize Gatekeeper, to define a list of parent filters and to choose whether or not to route calls to unresolved zones via the Cisco Proxy.

About Parent Filters

The LifeSize Gatekeeper sends an LRQ to the Parent Gatekeeper when the zone prefix of the call matches one of the defined parent filters. If the LifeSize Gatekeeper fails to match the zone prefix of the call with any of the defined parent filters, the LifeSize Gatekeeper either rejects the call or forwards the call according to the settings configured in the **Call Fallback** group box in the **Calls** section of the **Settings** tab. Where no filters are defined, the LifeSize Gatekeeper passes the call to the Parent Gatekeeper. The LifeSize Gatekeeper allows a maximum of ten parent filters.

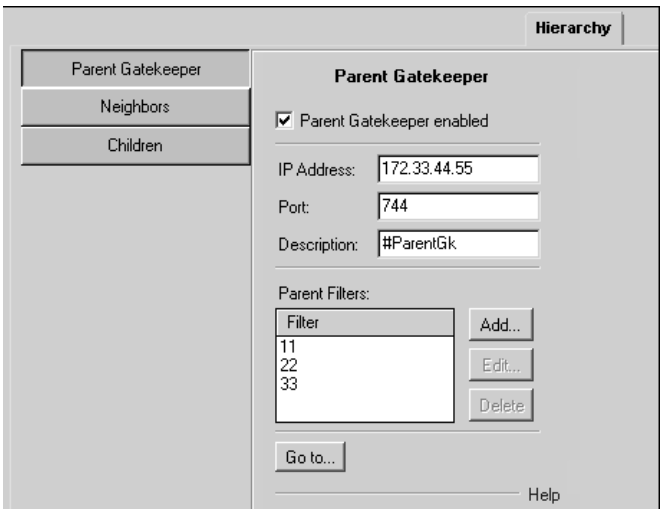

Figure 13-1 *Hierarchy Tab: Parent Gatekeeper*

WHAT YOU CAN CONFIGURE

The following options are available for configuring a Parent Gatekeeper:

Parent Gatekeeper enabled

When checked, enables you to define the LifeSize Gatekeeper as a Child of the configured Parent Gatekeeper.

IP Address

Type the IP address of the Parent Gatekeeper.

Port

Type the port number of the Parent Gatekeeper.

Description

Type a description of the Parent Gatekeeper (appears when you uncheck the **Use Central Database** option in the **Central Database** section of the **Settings** tab).

Gatekeeper ID

Displays the Parent Gatekeeper identifier (appears when you check the **Use Central Database** option in the **Central Database** section of the **Settings** tab).

Parent filters

Displays the list of defined parent filters. Parent filters instruct the LifeSize Gatekeeper whether or not to pass LRQ messages to the Parent Gatekeeper. If no filter is defined, the LifeSize Gatekeeper passes all LRQ messages to the Parent. For more information, see About Parent Filters on page 220.

Add

Click to add a new parent filter to the LifeSize Gatekeeper database. For more information, see Adding or Modifying a Parent Filter.

Edit

Double click a parent filter from the list, or select a parent filter from the list and click **Edit** to modify an existing parent filter. For more information, see Adding or Modifying a Parent Filter.

Delete

Select a parent filter from the list and click the **Delete** button to remove the specified parent filter from the list.

Note The **Add**, **Edit** and **Delete** options are disabled when you check the **Use Central Database** option in the **Central Database** section of the **Settings** tab.

Go to

Click to open the Administrator **Login** screen of the Parent LifeSize Gatekeeper.

Adding or Modifying a Parent Filter

To add a new parent filter, click **Add** to display the **Add Filter** dialog box. To modify an existing parent filter, double click the relevant parent filter from the list, or select a parent filter from the list and click **Edit** to display the **Edit Filter** dialog box.

The following options are available in the **Add Filter** and **Edit Filter** dialog box:

Filter

Type or modify the prefix that identifies the filter.

OK

Click to upload the new parent filter information to the LifeSize Gatekeeper database.

Neighbors

The **Neighbors** section of the **Hierarchy** tab enables you to view, configure and modify Neighbor Gatekeepers of the LifeSize Gatekeeper. For more information about Neighbor Gatekeepers, see the Neighbors Tab chapter.

Note When the **Connect to LDAP server** option is checked in the **LDAP** section of the **Settings** tab, the information displayed in the **Neighbors** section is read-only. For more information about LDAP, see LDAP on page 71.

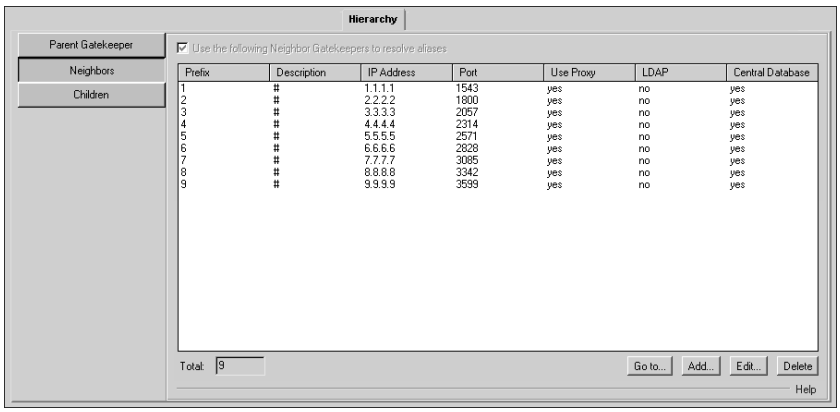

Figure 13-2 *Hierarchy Tab: Neighbors*

WHAT YOU SEE

The following information is displayed in the **Neighbors** section:

Use the following Neighbor Gatekeepers to resolve aliases

Check to instruct the LifeSize Gatekeeper to resolve aliases by sending a Location Request message (LRQ) to the Neighbor Gatekeepers currently listed in the LifeSize Gatekeeper database. For more information about the LRQ policy of the LifeSize Gatekeeper, see Resolution of Aliases on page 9.

Note This option is always checked when **Version 2** is selected in the **Dial Plan version** field in the **Basics** section of the **Settings** tab.

Table 13-1 *Neighbor Gatekeepers Configuration*

Field	Description
Prefix	Displays the zone prefix. For information on zone prefixes, see Zone Prefix 1 and 2 Service on page 157.
Description	Displays the Neighbor Gatekeeper description in free text. This field appears when the **Use Central Database** option is unchecked in the **Central Database** section of the **Settings** tab.
Gatekeeper ID	Displays the Neighbor Gatekeeper identifier. This field appears when the **Use Central Database** option is checked in the **Central Database** section of the **Settings** tab.
IP Address	Displays the IP address of the Neighbor Gatekeeper.
Port	Displays the port number of the Neighbor Gatekeeper.
Use Proxy	Indicates whether or not the LifeSize Gatekeeper routes all calls from this zone to the Neighbor Gatekeeper through the Cisco Proxy. For more information about the Cisco Proxy, see Cisco Proxy Support on page 6.
LDAP	Indicates whether or not the Neighbor Gatekeeper was retrieved from the LDAP server. For information on the LDAP server, see LDAP on page 71.

Table 13-1 *Neighbor Gatekeepers Configuration*

Field	Description
Central Database	Indicates whether or not the Neighbor Gatekeeper was retrieved from the Central Database. For information on the Central Database, see Central Database on page 87.

Total

Indicates the total number of Neighbor Gatekeepers currently listed in the LifeSize Gatekeeper database.

What You Can Configure

Go to

Click to open the Administrator **Login** screen of the specified Neighbor LifeSize Gatekeeper.

Add

Click to add a Neighbor Gatekeeper to the LifeSize Gatekeeper database. The LifeSize Gatekeeper allows a maximum of 100 Neighbor Gatekeepers. For more information, see Adding or Modifying a Neighbor Gatekeeper on page 226.

Edit

Double click a Neighbor Gatekeeper in the list, or select a Neighbor Gatekeeper and click **Edit** to modify the specified Neighbor Gatekeeper. For more information, see Adding or Modifying a Neighbor Gatekeeper.

Delete

Select a Neighbor Gatekeeper and click the **Delete** button to delete the specified Neighbor Gatekeeper from the LifeSize Gatekeeper database.

Note The **Add**, **Edit** and **Delete** buttons are disabled when you check the **Use Central Database** option in the **Central Database** section of the **Settings** tab.

Adding or Modifying a Neighbor Gatekeeper

To add a new Neighbor Gatekeeper, click **Add** to display the **Add Neighbor** dialog box. To modify an existing Neighbor Gatekeeper, double click the relevant Neighbor Gatekeeper in the **Neighbors** tab, or select a Neighbor Gatekeeper and click **Edit** to display the **Edit Neighbor** dialog box.

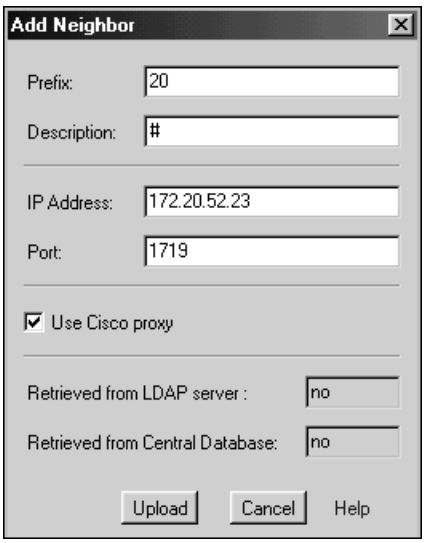

Figure 13-3 *Add Neighbor Dialog Box*

The following options are available in the **Add Neighbor** and **Edit Neighbor** dialog box:

Prefix

Type or modify the Neighbor Gatekeeper zone prefix. For information on zone prefixes, see Zone Prefix 1 and 2 Service on page 157.

Description

Type or modify the description of the Neighbor Gatekeeper.

IP Address

Type or modify the IP address of the Neighbor Gatekeeper.

Port

Type or modify the port number of the Neighbor Gatekeeper.

Use Cisco proxy

Check to instruct the LifeSize Gatekeeper to route all calls from this zone to the Neighbor Gatekeeper through the Cisco Proxy. For more information about the Cisco Proxy, see Cisco Proxy Support on page 6.

Retrieved from LDAP server (read only)

Indicates whether or not the Neighbor Gatekeeper was retrieved from the LDAP server. The configuration of Neighbor Gatekeepers retrieved from the LDAP server should be done through configuration of the information stored in the LDAP server and not through information stored in the LifeSize Gatekeeper. For more information on the LDAP server, see LDAP on page 71 and the Configuring the LDAP Server appendix.

Retrieved from Central Database (read only)

Indicates whether or not the Neighbor Gatekeeper was retrieved from the Central Database. When unchecked, indicates that the details of the Neighbor Gatekeeper were manually configured.

Upload

Click to add new Neighbor Gatekeeper information to the LifeSize Gatekeeper database.

CHILDREN

The **Children** section of the **Hierarchy** tab enables you to view, configure and modify Child Gatekeepers of the LifeSize Gatekeeper.

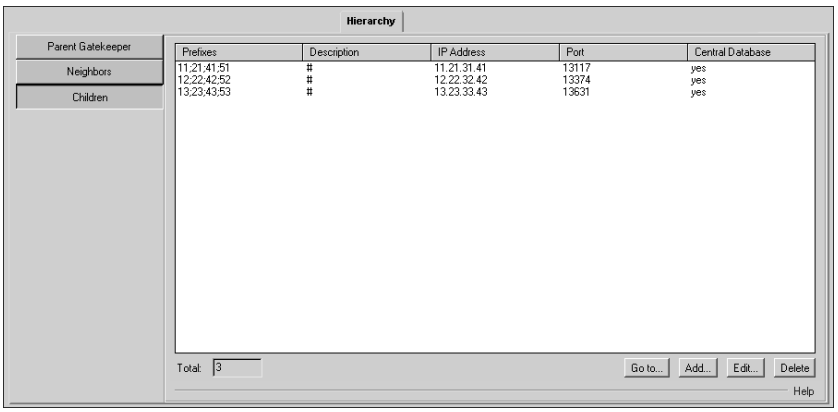

Figure 13-4 *Hierarchy Tab: Children*

WHAT YOU SEE

The following information is displayed in the **Children** section:

Table 13-2 *Child Gatekeepers Configuration*

Field	Description
Prefixes	Displays the zone prefix. For information on zone prefixes, see Zone Prefix 1 and 2 Service on page 157.
Description	Displays the Child Gatekeeper description in free text. This field appears when the **Use Central Database** option is unchecked in the **Central Database** section of the **Settings** tab.
Gatekeeper ID	Displays the Child Gatekeeper identifier. This field appears when the **Use Central Database** option is checked in the **Central Database** section of the **Settings** tab.
IP Address	Displays the IP address of the Child Gatekeeper.
Port	Displays the port number of the Child Gatekeeper.
Central Database	Indicates whether or not the Child Gatekeeper was retrieved from the Central Database. For information on the Central Database, see Central Database on page 87.

Total

Indicates the total number of Child Gatekeepers currently listed in the LifeSize Gatekeeper database.

What You Can Configure

Go to

Click to open the Administrator **Login** screen of the specified Child LifeSize Gatekeeper.

Add

Click to add a Child Gatekeeper to the LifeSize Gatekeeper database. The LifeSize Gatekeeper allows a maximum of 200 Child Gatekeepers. For more information, see Adding or Modifying a Child Gatekeeper on page 230.

Edit

Double click the relevant Child Gatekeeper in the list, or select a Child Gatekeeper and click **Edit** to modify the specified Child Gatekeeper. For more information, see Adding or Modifying a Child Gatekeeper on page 230.

Delete

Select a Child Gatekeeper and click the **Delete** button to delete the specified Child Gatekeeper from the LifeSize Gatekeeper database.

Note The **Add**, **Edit** and **Delete** options are disabled when you check the **Use Central Database** option in the **Central Database** section of the **Settings** tab.

Adding or Modifying a Child Gatekeeper

To add a new Child Gatekeeper, click **Add** to display the **Add Child** dialog box. To modify an existing Child Gatekeeper, double click the relevant Child Gatekeeper in the **Children** tab, or select a Child Gatekeeper and click **Edit** to display the **Edit Child** dialog box.

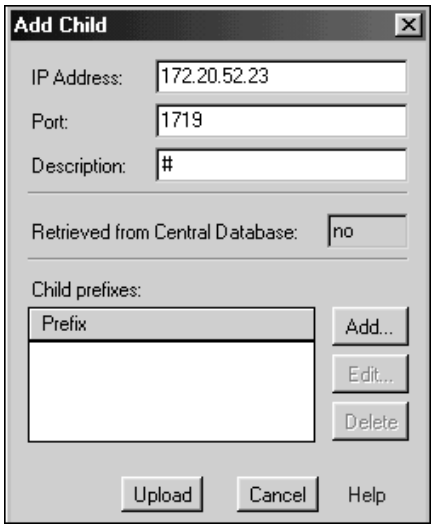

Figure 13-5 *Add Child Dialog Box*

The following options are available in the **Add Child** and **Edit Child** dialog box:

IP Address

Type or modify the IP address of the Child Gatekeeper.

Port

Type or modify the port number of the Child Gatekeeper.

Description

Type or modify the description of the Child Gatekeeper.

Retrieved from Central Database (read only)

When checked, indicates that the Child Gatekeeper was retrieved from the Central Database. When unchecked, indicates that the details of the Child Gatekeeper were manually configured.

Child prefixes

Displays the list of defined child prefixes. The LifeSize Gatekeeper sends an LRQ to the Child Gatekeeper when the zone prefix of the call matches one of the defined child prefixes. If the LifeSize Gatekeeper fails to match the zone prefix of the call with any of the defined Child Gatekeeper prefixes, the LifeSize Gatekeeper passes the call to a Neighbor Gatekeeper.

Add

Click to add a new child prefix to the LifeSize Gatekeeper database. For more information, see Adding or Modifying a Child Prefix on page 231.

Edit

Double click a child prefix from the list, or select a child prefix from the list and click **Edit** to modify an existing child prefix. For more information, see Adding or Modifying a Child Prefix on page 231.

Delete

Select a child prefix from the list and click the **Delete** button to remove an existing child prefix from the LifeSize Gatekeeper database.

Upload

Click the **Upload** button to add the Child Gatekeeper to the LifeSize Gatekeeper database.

Adding or Modifying a Child Prefix

To add a new child prefix to the LifeSize Gatekeeper database, click **Add** to display the **Add Prefix** dialog box. To modify an existing child prefix, double click the relevant child prefix from the list, or select a child prefix from the list and click **Edit** to display the **Edit Prefix** dialog box.

The following options are available in the **Add Prefix** and **Edit Prefix** dialog box:

Prefix

Type or modify the child prefix.

OK

Click to upload the new child prefix information to the LifeSize Gatekeeper database.

Children

14

EVENT LOG TAB

ABOUT THE EVENT LOG TAB

The **Event Log** tab displays a list of the reported alarm events.

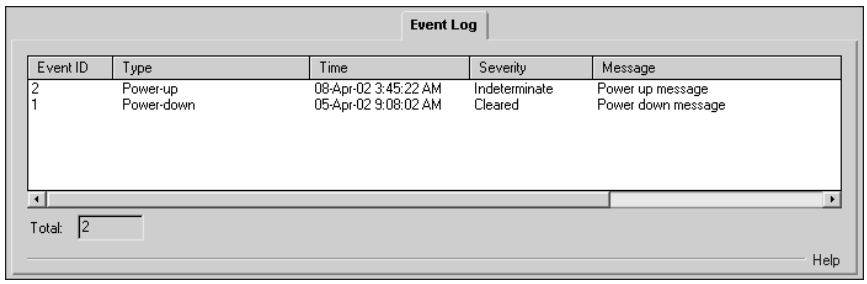

Figure 14-1 *Event Log Tab*

WHAT YOU SEE

The following information is displayed in the **Event Log** tab.

Table 14-1 *Event Log Tab Displayed Information*

Field	Description
Event ID	Displays the identifier for the specified alarm event.
Type	Displays the type of event.
Time	Displays the time at which the reported event occurred.
Severity	Displays the severity of the reported event.
Message	Displays the error message used to report the event.
Total	Displays the total number of reported alarm events.

Note The **Event Log** tab displays a list of the last 50 reported alarm events. The **Event Log** tab uses a cyclical mechanism that automatically refreshes the list every 10 seconds to show the previous 50 reported alarm events.

15

SECURITY PASSWORDS TAB

ABOUT THE SECURITY PASSWORDS TAB

The **Security Passwords** tab contains the user names and passwords for endpoints that are registered with the LifeSize Gatekeeper. The LifeSize Gatekeeper uses this information to encrypt all messages, including Gatekeeper Request messages (GRQ) and Registration Request messages (RRQ). You can use this tab to view, add to or modify endpoint details in the LifeSize Gatekeeper database.

Note The **Security Passwords** tab appears in the LifeSize Gatekeeper Administrator configuration interface only when you enable H.235 security in the **Security** section of the **Settings** tab.

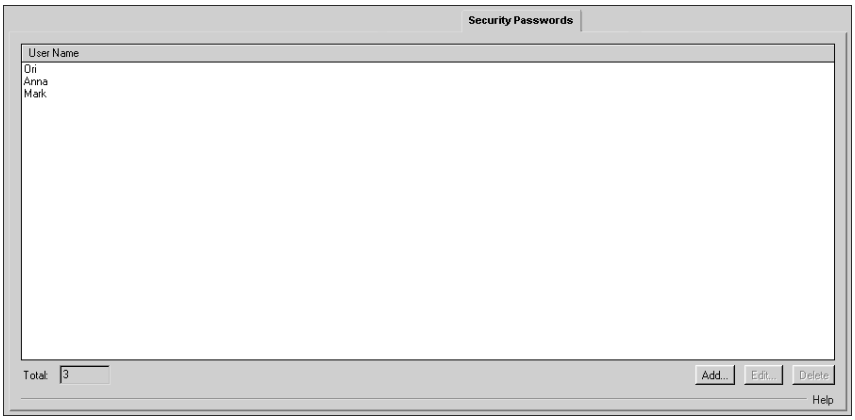

Figure 15-1 *Security Passwords Tab*

WHAT YOU SEE

The following information is displayed in the **Security Passwords** tab:

User Name

The H.235 user name of the endpoint that is registered with the LifeSize Gatekeeper.

Total

Indicates the total number of users currently registered with the LifeSize Gatekeeper.

WHAT YOU CAN CONFIGURE

Add

Click to add new user details to the LifeSize Gatekeeper database.

Edit

Double click the relevant entry in the list, or select the relevant entry and click **Edit** to modify existing user details in the LifeSize Gatekeeper database.

Delete

Select the relevant entry and click the **Delete** button to remove existing user details from the LifeSize Gatekeeper database.

Adding or Modifying User Details

To add new user details to the LifeSize Gatekeeper database, click **Add** to display the **Add User** dialog box. To modify existing user details, double click the required user profile, or select the required user profile and click **Edit** to display the **Edit User** dialog box.

The following options are available in the **Add User** and **Edit User** dialog box:

User name

Enter the user name for the endpoint registered with the LifeSize Gatekeeper.

Password

Enter the password for the user name registered with the LifeSize Gatekeeper.

Confirm password

Re-enter the password for the user name registered with the LifeSize Gatekeeper.

Upload

Click the **Upload** button to add the new user information to the LifeSize Gatekeeper database.

16

VERSION TAB

ABOUT THE VERSION TAB

The **Version** tab displays the version numbers of various system components.

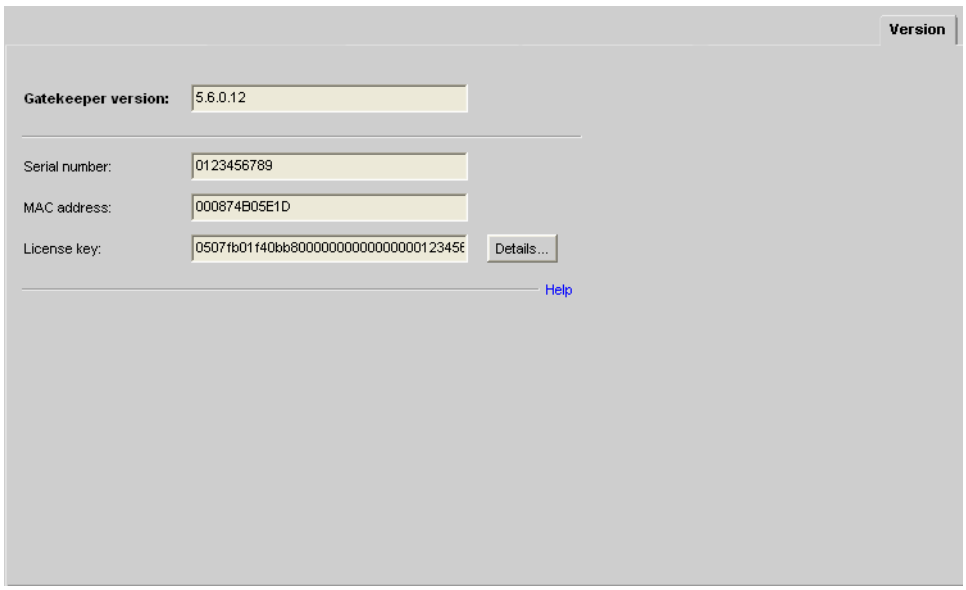

Figure 16-1 *Version Tab*

What You See

The following system component information is displayed in the **Version** tab:

Gatekeeper version

Displays the current LifeSize Gatekeeper version number.

Serial number

Displays the 10-digit serial number included in your LifeSize Gatekeeper license.

MAC address

Displays the current Media Access Control address (MAC address) included in your LifeSize Gatekeeper license key

License key

Displays the current LifeSize Gatekeeper license key.

Details

Click the **Details** button to open the **License Details** window for viewing licensing information.

Viewing License Details

The **License Details** window displays the following licensing information:

- The maximum number of calls allowed.
- The maximum number of registrations allowed.
- Whether the LifeSize Gatekeeper is a Primary or Secondary LifeSize Gatekeeper for Alternate Gatekeeper purposes.
- Whether or not the Central Database is enabled.
- Whether or not Third Party Call Control is enabled.
- Whether or not Child Gatekeeper usage is enabled.
- Whether or not the LifeSize Gatekeeper external API is enabled.
- Whether or not a connection to a RADIUS server is enabled.
- Whether or not management for subzone rules is enabled.

Configuring the LDAP Server

17

CONFIGURING THE LDAP SERVER

WHAT'S IN THIS CHAPTER

This chapter describes how to configure a Lightweight Directory Access Protocol (LDAP) server for the LifeSize Gatekeeper. LDAP supports directory operations between a client and a server residing on different machines. The main operations of the protocol are search, add, delete and modify.

The LifeSize Gatekeeper can connect to an LDAP server that has been configured to LifeSize Gatekeeper requirements. Once connected, the LifeSize Gatekeeper uses LDAP for directory services.

This chapter introduces you to the following:

- LDAP Basics
- Supported LDAP Servers
- Supported LDAP Schemas
- Inside the Gatekeeper Schema
- Configuration Options for Supported LDAP Servers
- LDAP Configuration Tool
- Automatic Configuration for Sun Java System, NDS or iPlanet Directory Server (Both Schemas)
- Automatic Configuration for Microsoft ADS (Both Schemas)
- Working with the Gatekeeper Schema
- Manually Configuring the OpenLDAP Server (Gatekeeper Schema)
- Manually Configuring the OpenLDAP Server (H.350 Schema)
- Binding the LifeSize Gatekeeper to the LDAP Server

LDAP Basics

A special LifeSize LDAP client module is used for retrieving information from a dedicated LDAP server, for permitting or denying a service (such as registration to the LifeSize Gatekeeper), or for routing calls.

The LDAP module defines entry structures, sets user and gatekeeper information in these structures, and stores them in an LDAP server. The information thus stored in the LDAP server is then used by the LifeSize Gatekeeper LDAP module for address resolution.

Supported LDAP Servers

The LifeSize Gatekeeper LDAP module supports the following LDAP servers:

- Sun Java System Directory Server 5.2 (formerly Sun ONE Directory Server 5.2) (http://wwws.sun.com/software/products/directory_srvr/home_directory.html)
- Netscape Directory Server 4.1
- iPlanet Directory Server 5.1 and 5.2
- Microsoft Active Directory Server 2000 and 2003 (http://www.microsoft.com/windowsserver2003/technologies/directory/activedirectory/default.mspx)
- OpenLDAP 2.0.27 (http://www.openldap.org/software/download)

Supported LDAP Schemas

The LifeSize Gatekeeper supports the following schema types:

- A proprietary LifeSize Gatekeeper schema.
- The ITU-T Recommendation H.350 schema.

Gatekeeper Schema

The Gatekeeper schema is a proprietary schema which enables you to

- Perform authentication according to endpoint alias and/or IP address.
- Locate and update endpoints, and to retrieve a list of Neighbor Gatekeepers from the LDAP server.

H.350 Schema

The ITU-T Recommendation H.350 schema is a schema for endpoints which support H.235 Annex D security, enabling you to

- Perform authentication according to the H.235 sender identifier and password.

  Authentication of non-H.235 endpoints is performed according to the endpoint name alias (the H.323 ID).
- Perform call authorization.

Note For more information on Recommendation H.350, see http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-H.350-200308-I.

Inside the Gatekeeper Schema

This section describes the content and structure of the LifeSize proprietary LDAP schema.

LDAP Tree

User and gatekeeper information is stored in the LDAP server in various trees. The Gatekeeper schema LDAP Tree consists of an H.323 zone root node with the following nodes:

- Static Information
- Online Information
- Gatekeeper List

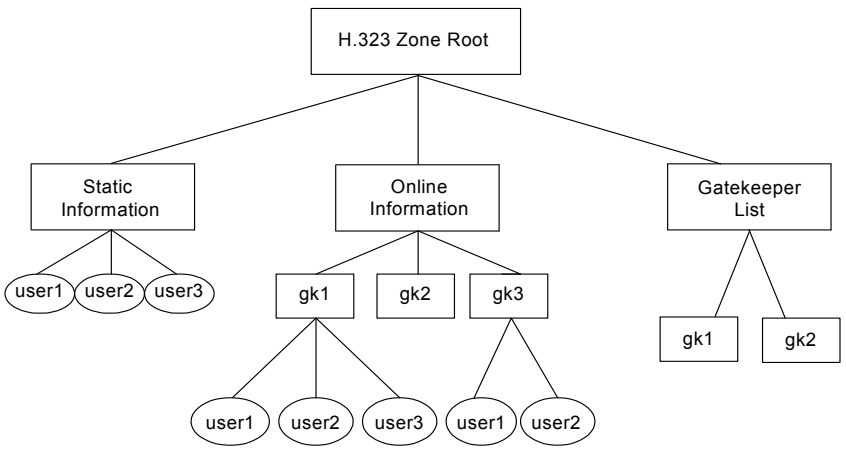

Figure 17-1 *LDAP Tree*

Static Information Tree

The Static Information Tree stores static information for each endpoint, such as user aliases, IP addresses, user logins and passwords, and a list of gatekeepers each endpoint has permission to access. An administrator or application configures and maintains this information. The LifeSize Gatekeeper LDAP module performs search, add, delete and modify operations.

Online Information Tree

The Online Information Tree stores online information and consists of sub-trees for each gatekeeper in the system. The tree stores the list of its online endpoints under each gatekeeper sub-tree when you check the **Update LDAP server with online information** option in the **LDAP** section of the **Settings** tab (see LDAP on page 71). The LifeSize Gatekeeper LDAP module maintains this tree and synchronizes the registrations with the list of users in the LDAP server under the corresponding LifeSize Gatekeeper entry. You enable maintenance and synchronization by defining entries for each LifeSize Gatekeeper under the *Online Information* directory using the **lsfolder** object class.

Gatekeeper List Tree

The Gatekeeper List Tree centralizes the details of the gatekeepers in the system. The object class for each gatekeeper entry is **lsgk**. For each gatekeeper, this tree stores:

- IP addresses (Call Signaling and RAS addresses).
- Gatekeeper identifier.
- Prefix.
- An indication of the gatekeeper routing mode (routed or direct).

Aside from this list, all references in the LDAP Tree to a gatekeeper will be to the gatekeeper identifier only. For instance, in the Static Information Tree, the allowed gatekeeper list of the user consists solely of such gatekeeper identifiers. The Gatekeeper List Tree supplies the detailed information of those gatekeepers.

Configuration Options for Supported LDAP Servers

This section describes the configuration options that are available for each of the supported LDAP servers.

Automatic Configuration

Use the LDAP Configuration Tool to automatically configure the following directory servers to work with either the Gatekeeper schema or the H.350 schema:

- Sun Java System Directory Server 5.2 (formerly Sun ONE Directory Server 5.2)
- Netscape Directory Server
- iPlanet Directory Server
- Microsoft Active Directory Server

For more information, see LDAP Configuration Tool on page 247.

Manual Configuration

You must manually configure **OpenLDAP** server to work with either the Gatekeeper schema or the H.350 schema.

For more information, see Manually Configuring the OpenLDAP Server (Gatekeeper Schema) on page 257 and Manually Configuring the OpenLDAP Server (H.350 Schema) on page 260.

LDAP Configuration Tool

The LDAP Configuration Tool is an external Windows-based application which runs either on the LDAP server or on a remote computer. The Configuration Tool allows the user to automatically create the LDAP Tree structure required by the LifeSize Gatekeeper on the LDAP server.

The LDAP Configuration Tool enables you to automatically configure the following directory servers to use either the Gatekeeper schema or the H.350 schema:

- Sun Java System Directory Server 5.2 (formerly Sun ONE Directory Server 5.2)
- Netscape Directory Server
- iPlanet Directory Server
- Microsoft Active Directory Server

Accessing the LDAP Configuration Tool

This section describes how to access the LDAP Configuration Tool.

To access the LDAP Configuration Tool

1. Copy the *LifeSize_GK_Setup.exe* file from the LifeSize Gatekeeper CD-ROM to your local machine, and then run the file.
2. Click **Next**.

   The **License Agreement** dialog box displays.
3. Select the **I accept the terms of the license agreement** option, and click **Next** to continue.

   The **Setup Type** dialog box displays.
4. Select the **Custom** option, and click **Next**.

   The **Choose Destination Location** dialog box displays.
5. Click **Next** to continue.

   The **Select Features** dialog box displays.
6. Ensure that the LifeSize Gatekeeper option is checked. This is the core LifeSize Gatekeeper component and this option is enabled by default.
7. Check the LifeSize **LDAP Configuration Utility** option to automatically create the LDAP Tree structure required by the LifeSize Gatekeeper on an LDAP server.
8. Click **Next**.

   The **License Key** dialog box displays.
9. If you have already received a license key from LifeSize Customer Support, select the **I have a license key** option and copy your license key into the **Please enter your license key** text box. Then click **Next**.

   If you have not already received a license key from LifeSize Customer Support, select the **I want to evaluate** LifeSize Gatekeeper option. Then click **Next**.

   The **Summary** screen displays.
10. Click **Next** to continue.

    Installation begins and the installation status screen displays.

    When the installation process finishes, the **Installation Complete** screen displays.

11 Click **Finish** to exit the installation wizard.

12 From the **Start** menu, go to **Programs > LifeSize > Gatekeeper > LDAP Configuration Tool**.

13 The **Login** dialog box displays.

Automatic Configuration for Sun Java System, NDS or iPlanet Directory Server (Both Schemas)

This section describes how you configure the LDAP Configuration Tool to enable the Sun Java System Directory Server 5.2 (formerly Sun ONE Directory Server 5.2), the Netscape Directory Server (NDS), or the iPlanet Directory Server to work with either the Gatekeeper schema or the H.350 schema.

To configure the LDAP Configuration Tool for Sun Java System Directory Server 5.2, Netscape Directory Server and iPlanet Directory Server

1 Type the address of the LDAP server in the **Server address** field of the **Login** dialog box.

The default setting is *localhost*. All server addresses entered are stored and appear in the drop-down list.

Note If the LDAP server you want to configure uses a non-standard port (not port 389) you can specify the port after the host name using a semicolon. For example, *localhost:12345* if the port value is 12345.

---

2 Type the LDAP server user identifier in the **User ID** field.

The default setting is *cn=Directory Manager*. All user identifiers entered are stored and appear in the drop-down list.

Note We recommend that you use the default setting in the **User ID** field.

---

3. Type the LDAP server password defined during LDAP installation in the **Password** field.
4. Click **OK** to connect to the LDAP server.

   The LDAP Configuration Tool dialog box displays.
5. Type the root node of the required LDAP Tree in the **Base DN** field.

   The default root node is *lifesize.com*.

Note

- When working with the Gatekeeper schema, the LDAP Configuration Tool automatically adds the prefix *o=* to the **Base DN** field.
- When working with the H.350 schema, you must add a prefix to the root node specified in the **Base DN** field.
- For example
  - If you use the default root node *o=lifesize.com* with the Gatekeeper schema, type only *lifesize.com.*
  - If you use the default root node with the H.350 schema, type *o=lifesize.com*, where *o=* is the prefix.

6. Select the required schema from the drop-down list in the **Type** field. Then click **Check/Create**.

   The LDAP Configuration Tool checks whether or not the LDAP schema and the relevant folders exist on the LDAP server.

LDAP Schema and Relevant Folders Exist on the Server

This section is a continuation of the Automatic Configuration for Sun Java System, NDS or iPlanet Directory Server (Both Schemas) section. This section describes how you proceed when the LDAP schema and the relevant folders exist on the LDAP server.

To configure the LDAP Configuration Tool for Sun Java System Directory Server 5.2, Netscape Directory Server and iPlanet Directory Server when the schema exists on the server

1. Click the **Check/Create** button.

   The *The LDAP Schema is OK* message displays.

2 Click the **OK** button.

The LDAP Configuration Tool dialog box displays with all LDAP Tree component **Status** settings set to **OK**.

3 Click **Close** to complete the automatic configuration.

LDAP Schema and Relevant Folders Do Not Exist on the Server

This section is a continuation of Automatic Configuration for Sun Java System, NDS or iPlanet Directory Server (Both Schemas). This section describes how you proceed when the LDAP schema and the relevant folders do not exist on the LDAP server.

To configure the LDAP Configuration Tool for Sun Java System Directory Server 5.2, Netscape Directory Server and iPlanet Directory Server when the schema is not on the server

1 Click the **Check/Create** button.

The *The LDAP Schema must be updated! Do you want to update it now?* message displays.

In addition, the **Status** settings in the LDAP Configuration Tool dialog box indicate which of the components of the LDAP Tree (**Attributes**, **Object classes**, **Naming context** and **Folders**) are missing.

2 Click **Yes** to respond to the *The LDAP Schema must be updated! Do you want to update it now?* message.

The **Status** settings for **Naming context** and **Folders** in the LDAP Configuration Tool dialog box change to **OK**.

3 Click **Close** to complete the automatic configuration.

Automatic Configuration for Microsoft ADS (Both Schemas)

This section describes how you configure the LDAP Configuration Tool to enable the Microsoft Active Directory Server (ADS) to work with the Gatekeeper schema.

To configure the LDAP Configuration Tool for the Microsoft Active Directory Server

1. Type the address of the LDAP server in the **Server address** field of the **Login** dialog box.

   The default setting is *localhost*. All server addresses entered are stored and appear in the drop-down list.
2. Type the LDAP server user identifier in the **User ID** field. For example, *cn=administrator,cn=users,dc=gatekeeper,dc=com* where *dc=gatekeeper,dc=com* represents the domain of the LDAP server host (*gatekeeper.com*).
3. Type the LDAP server password defined during LDAP installation in the **Password** field.
4. Click **OK** to connect to the LDAP server.

   The LDAP Configuration Tool dialog box displays.
5. Type the root node of the required LDAP Tree in the **Base DN** field.

   The default root node is *lifesize.com*.

Note The string that you type in the **Base DN** field must end with the computer domain used in the **User ID** field. For example, if you typed *cn=administrator,cn=users,dc=gatekeeper,dc=com* in the **User ID** field, the string that you type in the **Base DN** field must end with *,dc=gatekeeper,dc=com*.

---

6. Select LifeSize from the drop-down list in the **Type** field. Then click **Check/Create**.

   The LDAP Configuration Tool checks whether or not the LDAP schema and the relevant folders exist on the LDAP server.

- If yes, the *The LDAP Schema is OK* message displays. For more information, see LDAP Schema and Relevant Folders Exist on the Server on page 250.
- If no, the LDAP Configuration Tool attempts to configure the schema and create the relevant folders under the specified Base DN. For more information, see LDAP Schema and Relevant Folders Do Not Exist on the Server on page 251.

WORKING WITH THE GATEKEEPER SCHEMA

This section describes how to work with the Sun Java System Directory Server 5.2 (formerly Sun ONE Directory Server 5.2), the Netscape Directory Server 4.1, the iPlanet Directory Server 5.1 and the Microsoft Active Directory Server using the Gatekeeper schema.

ACCESSING THE LDAP TREE

This section describes the procedure for accessing the LDAP Tree on the LDAP server after you have completed the configuration described in Automatic Configuration for Sun Java System, NDS or iPlanet Directory Server (Both Schemas) on page 249 or in Automatic Configuration for Microsoft ADS (Both Schemas) on page 252. The LDAP Tree is known as the **h323 zone** tree on the LDAP server.

To access the LDAP Tree on the LDAP server

1. Log in to the LDAP server console using the *cn=Directory Manager* user identifier and the same password as used on installation.

   The **Console** window displays.
2. In the **Console** tab, double click the icon representing the root node (<*root node*>). The default root node name is **lifesize.com**.
3. From <*root node*> click the icon representing the name of the host computer on which the LDAP server is installed (<*server host*>) and then select **Server Group > Directory Server (<server host>)**.

   The **Task**, **Configuration**, **Directory** and **Status** tabs display.
4. From the **Directory** tab select **<server host>:389** | **<root node>** | **h323 zone** by double clicking on each folder.

   The **static information**, **online information** and **gk list** folders appear.

Modifying the LDAP Tree

This section describes the procedure for modifying the LDAP Tree. You can add new entries to any of the nodes beneath the root node.

Before You Begin

There are some minor differences between Netscape Directory Server 4.1 and iPlanet Directory Server 5.1. The following sections document the Netscape server. The differences are as follows:

- The Netscape **Property Editor - New** dialog box is called simply **Property Editor** in the iPlanet server.
- The Netscape **View** menu box is a group box within the **Property Editor** dialog box in the iPlanet server.
- The Netscape server requires you to right click specified fields to add an additional field of the same type. In the iPlanet server, place the cursor in the specified field and select **Add Value** to add similar fields.
- To access the **Add Attribute** list in the iPlanet server, select **Add Attribute** in the **Property Editor** dialog box. For instructions on adding attributes to the Netscape server, see To activate optional Property Editor fields on page 255.

To add a new entry to the Static Information Tree

1. Enter the Directory Server of the LDAP server console and select the **Directory** tab. Double click the root node icon (**lifesize.com**), and then select and double click **h323 zone**.
2. Place the cursor on **static information** and right click. From the drop-down list select **New** and then **Object** (or **Other**).
3. From the **New object** drop-down list, select **lsuserstatic** and double click (or press **OK**).
4. In the **Property Editor - New** dialog box, select the **View** menu and then **Show all attributes** (if using Netscape Directory Server). Type the user alias in the **lsuseralias** field. Enter *TEL:*, *EMAIL:*, *URL:* or *NAME:* before each alias according to the alias type.

   To add an additional user alias in Netscape Directory Server, right click the **lsuseralias** field and select **Add value**. An additional **lsuseralias** field appears. Repeat the process to add further user aliases.

   To add an additional user alias in iPlanet Directory Server, click the **lsuseralias** field, then click the **Add Value** button. An additional **lsuseralias** field appears. Repeat the process to add further user aliases.

5 If using Netscape Directory Server, type the gatekeeper identifier in the **lsgkid** field. To add an additional gatekeeper identifier to which the user has access, right click the **lsgkid** field and select **Add value**.

An additional **lsgkid** field appears. Repeat the process to add further gatekeeper identifiers.

If using iPlanet Directory Server, click **Add Attribute** and select **lsgkid** from the **Add Attribute** list. Type the gatekeeper identifier in the **lsgkid** field. To add an additional gatekeeper identifier, click the **lsgkid** field, then click the **Add Value** button.

An additional **lsgkid** field appears. Repeat the process to add further user aliases.

6 Type the IP address and Call Signaling port in the **lsuseripcs** field (e.g. 172.23.1.10:1720), the IP address and RAS port in the **lsuseripras** field (e.g. 172.23.1.10:1719), and, optionally, the user password in the **lsuserpsswd** field.

To activate any of these fields, see To activate optional Property Editor fields on page 255.

Note To allow access from an endpoint to a LifeSize Gatekeeper that is bound to an LDAP server, add the endpoint details and the gatekeeper identifier to the Static Information Tree.

Note Define static endpoint e-mail aliases in the LDAP server using lower case only, regardless of how you define the e-mail alias in the endpoint itself. For example, define EMAIL:abc@company, and not EMAIL:ABC@Company. You should write the alias type “EMAIL” in upper case letters.

To activate optional Property Editor fields

1 Right click the **Property Editor - New** dialog box to open the **Add Attribute** window.

2 Select the required attribute from the list and click **OK**.

The selected attribute appears as a field in the **Property Editor - New** dialog box.

To add a new entry to the Online Information Tree

1. Enter the Directory Server of the LDAP server console and select the **Directory** tab. Double click <*root node*> (**lifesize.com** is the default root node name), and then select and double click **h323 zone**. Place the cursor on **online information** and right click.
2. From the drop-down list, select **New** and then **Object** (or **Other**).
3. From the **New object** dialog box list, select **lsfolder** and double click.

Note Define an **lsfolder** for each LifeSize Gatekeeper that works with the **Update LDAP server with online information** option in the **LDAP** section of the LifeSize Gatekeeper **Settings** tab (see LDAP on page 71).

4. In the **Property Editor - New** dialog box, type the gatekeeper identifier in the **Full name** field.

Note The gatekeeper identifier that you enter in the **Full name** field must be the same as the gatekeeper identifier in the **Gatekeeper ID** field in the **Basics** section of the LifeSize Gatekeeper **Settings** tab. Each new entry to the Online Information Tree must have a unique gatekeeper identifier.

To add a new entry to the Gatekeeper List Tree

1. Enter the Directory Server of the LDAP server console and select the **Directory** tab. Double click <*root node*> (**lifesize.com** is the default root node name), and then select and double click **h323 zone**.
2. Place the cursor on **gk list** and right click. From the drop-down list select **New** and then **Object** (or **Other**). From the **New object** drop-down list, select **lsgk** and double click.
3. In the **Property Editor-New** dialog box, select the **View** menu and then **Show all attributes** (if using Netscape Directory Server). Type the gatekeeper identifier in the **lsgkid** field.

Note The gatekeeper identifier that you enter in the **lsgkid** field must be the same as the gatekeeper identifier in the **Gatekeeper ID** field in the **Basics** section of the **Settings** tab. Each new entry to the Gatekeeper List Tree must have a unique gatekeeper identifier.

4 Type the IP address and Call Signaling port (1720) in the **lsgkipcs** field (e.g. 172.23.1.10:1720), the IP address and RAS port (1719) in the **lsgkipras** field (e.g. 172.23.1.10:1719), and the routing mode in the **lsgkmode** field. For Direct Mode, type **direct**. For Q.931 Mode, type **routed**. For Q.931 and H.245 Mode, type **routed**.

5 Optionally, type the gatekeeper description string in the **lsgkdesc** field and the relevant prefix in the **lsgkprefix** field.

To activate any of these fields, see To activate optional Property Editor fields on page 255.

Note You must add gatekeepers to the Gatekeeper List Tree if you are using the **Retrieve Neighbor Gatekeeper list every *n* seconds** option in the **LDAP** section of the LifeSize Gatekeeper **Settings** tab (see LDAP on page 71).

Manually Configuring the OpenLDAP Server (Gatekeeper Schema)

- Adding Entries to the LDAP Tree on page 257
- Modifying Entries in the LDAP Tree on page 259
- Deleting Entries from the LDAP Tree on page 260
- Viewing the Error Log on page 260

Adding Entries to the LDAP Tree

This section describes the procedure for adding entries to the LDAP Tree using the LDAP Browser\Editor.

Before You Begin

Before adding entries of object classes defined especially for the LifeSize Gatekeeper (**lsfolder**, **LSgk** or **lsuserstatic**) for the first time, you must create a template for each object class.

To create an object class template

1 Select one of the entries already defined under the appropriate folder in the LDAP Tree.

For example, to create a template for the **LSgk** object class, select an entry already defined under the **cn=gk list** folder.

2. From the **Edit** menu, select **Create Template**.

   Templates are automatically saved to *LdapBrowser\templates\templates.config* and a new file is created for each new template containing the required and optional attributes of the object class.

To add a new entry to the Static Information Tree

1. Select the **cn=static information** folder in the LDAP Tree.
2. In the **Edit** menu, select **Add Entry** and then **lsuserstatic**.

   The **Create New 'lsuserstatic' Entry** dialog box displays.
3. Type a new alias in the **lsuseralias** field and amend the *LSuserAlias=* string in the **dn** field.
4. Type the gatekeeper identifier in the **lsgkid** field.
5. Optionally, type the IP address and Call Signaling port in the **lsuseripcs** field (e.g. 172.23.1.10:1720), and the IP address and RAS port in the **lsuseripras** field (e.g. 172.23.1.10:1719).
6. Click **Apply** to complete the process.

To add a new entry to the Online Information Tree

1. Select the **cn=online information** folder in the LDAP Tree.
2. In the **Edit** menu, select **Add Entry** and then **lsfolder**.

   The **Create New 'lsfolder' Entry** dialog box displays.
3. Type a new gatekeeper identifier in the **cn** field and amend the *newlsfolder* string in the **dn** field.
4. Click **Apply** to complete the process.

Note After you have prepared the **lsfolder** entry in the LDAP Tree, the LifeSize Gatekeeper automatically updates online registration information.

To add a new entry to the Gatekeeper List Tree

1. Select the **cn=gk list** folder in the LDAP Tree.
2. In the **Edit** menu, select **Add Entry** and then **LSgk**.

   The **Create New 'LSgk' Entry** dialog box displays.

3 Type the IP address and RAS port in the **lsgkipras** field (e.g. 172.23.1.10:1719), and the IP address and Call Signaling port in the **lsgkipcs** field (e.g. 172.23.1.10:1720).

4 Type the mode in the **lsgkmode** field. For Direct Mode, type **direct**. For Q.931 Mode, type **routed**. For Q.931 and H.245 Mode, enter **routed**.

5 Type the gatekeeper identifier in the **lsgkid** field.

6 Optionally, type the gatekeeper description string in the **lsgkdesc** field, and the gatekeeper prefix in the **lsgkprefix** field.

7 Click **Apply** to complete the process.

Note After modifying the database, you can save the new database to a different *.ldif* file by using the **Export** option from the **LDIF** menu.

MODIFYING ENTRIES IN THE LDAP TREE

This section describes the procedure for modifying entries in the LDAP Tree using the LDAP Browser\Editor.

To modify an entry in the LDAP Tree

1 Select the required entry, and then select **Edit Entry** from the **Edit** menu.

The **Edit** dialog box displays.

2 Modify the existing attribute settings as required.

3 Click **Apply**.

To add an attribute to an entry in the LDAP Tree

1 Select the required entry, and then select **Edit Entry** from the **Edit** menu.

The **Edit** dialog box displays.

2 From the **Edit** menu, select **Add Attribute**.

The **Add attribute** dialog box displays.

3 Type the required attribute name and click **OK** to return to the **Edit** dialog box.

4 Click **Apply**.

Deleting Entries from the LDAP Tree

This section describes the procedure for deleting entries from the LDAP Tree using the LDAP Browser\Editor.

To delete an entry from the LDAP Tree

1. Select the required entry and click **Delete** on your keyboard.

   or

2. Select the required entry, and then select **Delete Entry** from the **Edit** menu.

   The **Delete Entry** dialog box displays.

3. If you wish to delete all the entries under the specified entry, check the **with children** checkbox.
4. Click **Delete**.

Viewing the Error Log

If an operation such as adding, modifying or deleting an LDAP Tree entry fails, you can view error details in the LDAP Browser\Editor error log.

To view the LDAP Browser\Editor error log

Select **View error log** from the **View** menu. The error log displays.

Manually Configuring the OpenLDAP Server (H.350 Schema)

This section describes how to configure the OpenLDAP Server 2.0.27 on a Linux platform to work with the LifeSize Gatekeeper using the ITU-T Recommendation H.350 schema.

Note For more information on Recommendation H.350, see http://www.itu.int/rec/recommendation.asp?type=items&lang=e&parent=T-REC-H.350-200308-I.

- Adding Entries to the LDAP Tree on page 261
- Modifying Entries in the LDAP Tree on page 263
- Deleting Entries from the LDAP Tree on page 263
- Viewing the Error Log on page 263

Adding Entries to the LDAP Tree

This section describes the procedure for adding entries to the LDAP Tree using the LDAP Browser\Editor.

Before You Begin

For the LifeSize Gatekeeper to work with the H.350 schema, you must define entries which represent H.323 endpoints in the LDAP server under the **ou=h323Identity** folder. Each entry belongs to both the **h323Identity** and **h235Identity** object classes, as defined in the H.350 specification.

Before adding entries for the first time, you must create a template for each object class.

To create an object class template

1. Select one of the entries already defined under the **ou=h323Identity** folder in the LDAP Tree.
2. From the **Edit** menu, select **Create Template**.

   The Create Template dialog box displays.

   Select either **h323Identity** or **h235Identity** from the drop-down list

   The **h235Identity** object class template automatically contains the **h323Identity** object class, and vice versa. There is, therefore, no need to create a separate template for each object class.

   Templates are automatically saved to *LdapBrowser\templates\templates.config* and a new file is created for each new template containing the required and optional attributes of the object class.

To add a new entry to the LDAP Tree

1. Select the **ou=h323identity** folder in the LDAP Tree.
2. In the **Edit** menu, select **Add Entry** and then **h323Identity** (or **h235Identity**).

   The **Create New 'h323Identity'** (or **'h235Identity'**) **Entry** dialog box displays.
3. Type a unique string (for example, a unique number) in the **commUniqueID** field.

4 In the **dn** field, amend the displayed string to "*commUniqueID=xxx,"* where *xxx* represents the new value in the **commUniqueID** field.

Note You must replace the "*commUniqueID="* string only up to the first comma (,). For example, if the displayed string is *commUniqueID=newh235Identity,ou=h232Identity,dc=gatekeeper,dc=com,* and you have typed "30" in the **commUniqueID** field, you must replace *newh235Identity* with 30. The resulting string is *commUniqueID=30,ou=h232Identity,dc=gatekeeper,dc=com*

---

5 Type the endpoint H.235 sender identifier in the **h235IdentityEndpointID** field.

If the endpoint does not support H.235 Annex D, type the endpoint name alias (H.323 ID).

6 Type the endpoint H.235 password in the **h235IdentityPassword** field to use the LifeSize Gatekeeper authentication feature with the H.350 schema.

You do not need to fill this field for endpoints that do not support H.235 Annex D.

7 Type the endpoint service level in the **h323IdentityServiceLevel** field to use the LifeSize Gatekeeper authorization feature with the H.350 schema.

The LifeSize Gatekeeper uses this attribute to define which endpoints are members of a specified group.

You must define a group with the same name as the endpoint service level in the **Groups** section of the LifeSize Gatekeeper **Endpoints** tab (see Groups on page 140).

8 If you choose to register endpoints using the **LDAP aliases** or **Online and LDAP aliases** settings in the **Register endpoints with** field in the **LDAP** section of the LifeSize Gatekeeper **Settings** tab (see LDAP on page 71), define the endpoint aliases in the following fields:

- **h323Identityh323-ID**—For name aliases.
- **h323IdentitydialedDigits**—For E.164 aliases.
- **h323Identityemail-ID**—For e-mail aliases.
- **h323IdentityURL-ID**—For URL aliases.
- **h323IdentitytransportID**—For transport address aliases.

- **h323IdentitypartyNumber**—For party number aliases.

9 Optionally, you can type the endpoint type in the **h323IdentityEndpointType** field, and the gatekeeper domain in the **h323IdentityGkDomain** field. The LifeSize Gatekeeper does not use these fields.

10 Click **Apply** to complete adding the entry.

Note After modifying the database, you can save the new database to a different *.ldif* file by using the **Export** option from the **LDIF** menu.

To add an attribute to an entry in the LDAP Tree

1 Select the required entry, and then select **Edit Entry** from the **Edit** menu.

The **Edit** dialog box displays.

2 From the **Edit** menu, select **Add Attribute**.

The **Add attribute** dialog box displays.

3 Type the required attribute name and click **OK** to return to the **Edit** dialog box.

4 Click **Apply**.

Modifying Entries in the LDAP Tree

The procedure for modifying entries in the LDAP Tree using the LDAP Browser\Editor is described at Modifying Entries in the LDAP Tree on page 259.

Deleting Entries from the LDAP Tree

The procedure for deleting entries from the LDAP Tree using the LDAP Browser\Editor is described at Deleting Entries from the LDAP Tree on page 260.

Viewing the Error Log

The procedure for viewing error details in the LDAP Browser\Editor error log is described at Viewing the Error Log on page 260.

Binding the LifeSize Gatekeeper to the LDAP Server

This section describes the procedure for binding the LifeSize Gatekeeper to the LDAP server. For more information about configuring LifeSize Gatekeeper LDAP options, see LDAP on page 71.

To bind the LifeSize Gatekeeper to the LDAP server

1. Select **Everyone** in the **Who can register** option in the **Basics** section of the **Settings** tab.
2. Check the **Connect to LDAP server** option in the **LDAP** section of the **Settings** tab.
3. Type the LDAP server IP address or the domain name in the **Server address** field.
4. The default value in the **Port** field for the LDAP protocol is *389*.
5. Type the user name in the **User** field and the password in the **Password** field.
6. Type the base DN in the **Base DN** field.
7. Select the **Upload** button.

Note When working with the Gatekeeper schema, the LifeSize Gatekeeper automatically adds the prefix *o=* to the Base DN. For example, if you type *lifesize.com*, the LifeSize Gatekeeper modifies the Base DN string to *o=lifesize.com*.

APPENDICES

APPENDIX A

ADDITIONAL INSTALLATION INFORMATION

WHAT'S IN THIS APPENDIX

This appendix provides additional installation information to enable you to meet the minimum requirements for the LifeSize Gatekeeper, including the following:

- Installing the SNMP Service (Windows 2000/2003)
- Configuring the SNMP Service (Windows 2000/2003)
- Installing IIS 4 Subcomponents (Windows 2000)
- Installing IIS 4 Subcomponents (Windows 2003)
- Configuring IIS 4 Subcomponents (Windows 2000/2003)

Installing the SNMP Service (Windows 2000/2003)

This procedure describes how you install the Microsoft SNMP service on the Windows 2000 and 2003 operating systems.

To install the Microsoft SNMP service on Windows 2000 and 2003

1. From the **Start** menu of the target device, select **Settings > Control Panel > Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.

   The **Windows Components Wizard** dialog box displays.
3. Check the **Management and Monitoring Tools** checkbox and click **Details**.

   The **Management and Monitoring Tools** dialog box displays.
4. Verify that **Simple Network Management Protocol** is checked. Click **OK**.
5. Click **Next**, wait for the installation to complete and click **Finish**.

Note During the installation you may be prompted to insert a Microsoft CD-ROM. Insert the CD-ROM or click **OK** to copy the I386 files from an alternate location.

Configuring the SNMP Service (Windows 2000/2003)

This procedure describes how you configure the Microsoft SNMP service on the Windows 2000 and 2003 operating systems.

To configure the Microsoft SNMP service on Windows 2000 and 2003

1. From the **Start** menu of the target device, select **Settings** > **Control Panel > Administrative Tools > Services** and double click the SNMP service, or

   Right click **SNMP** from the list of services and click **Properties**.

   The **SNMP Service Properties (Local Computer)** dialog box (Figure A-1 on page 269) displays.
2. Select the **Security** tab.

3 Select **public** in the **Accepted community names** list box and click the **Edit** button.

4 Select **READ CREATE** from the drop-down list and click **OK**.

READ CREATE appears in the **Rights** column of the **Accepted community names** list box.

5 Click **OK** again.

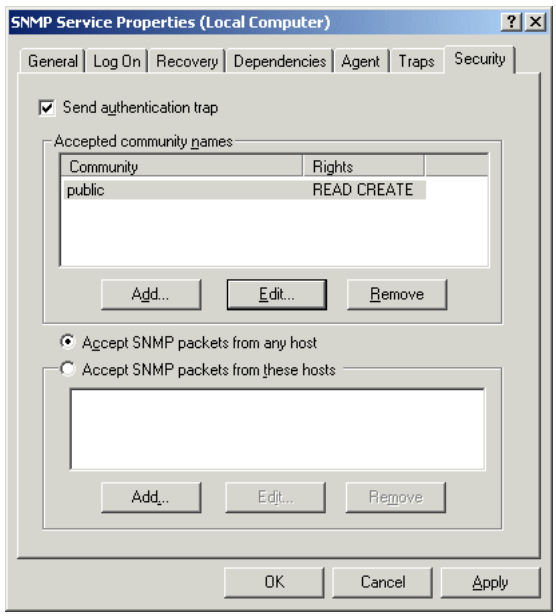

Figure A-1 *SNMP Service Properties (Local Computer) Dialog Box*

INSTALLING IIS 4 SUBCOMPONENTS (WINDOWS 2000)

This procedure describes how you install IIS 4 subcomponents on the Windows 2000 operating system.

To install IIS 4 subcomponents on Windows 2000

1. From the **Start** menu, select **Settings > Control Panel > Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.

   The **Windows Components Wizard** dialog box (Figure A-2) displays.

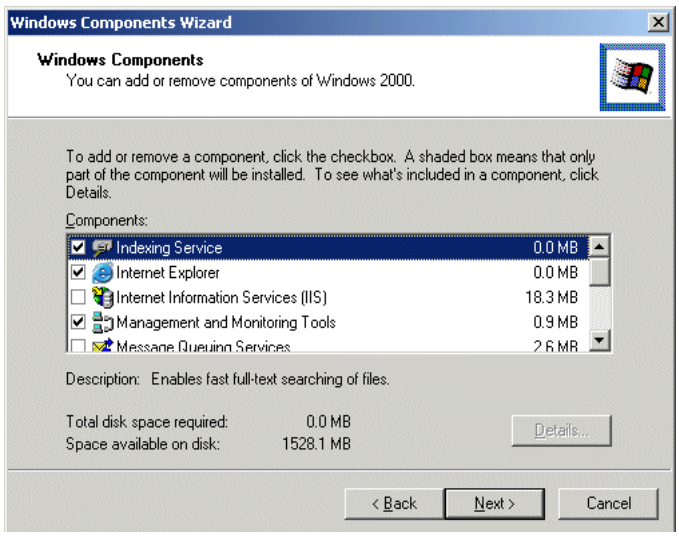
Windows Components Wizard
Windows Components
You can add or remove components of Windows 2000.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Indexing Service 0.0 MB
Internet Explorer 0.0 MB
Internet Information Services (IIS) 18.3 MB
Management and Monitoring Tools 0.9 MB
Message Queuing Services 2.6 MB
Description: Enables fast full-text searching of files.
Total disk space required: 0.0 MB
Space available on disk: 1528.1 MB
Details...
< Back
Next >
Cancel

Figure A-2 *Windows Components Wizard Dialog Box*

3 Select **Internet Information Services (IIS)** and click **Details**.

The **Internet Information Services (IIS)** dialog box (Figure A-3) displays.

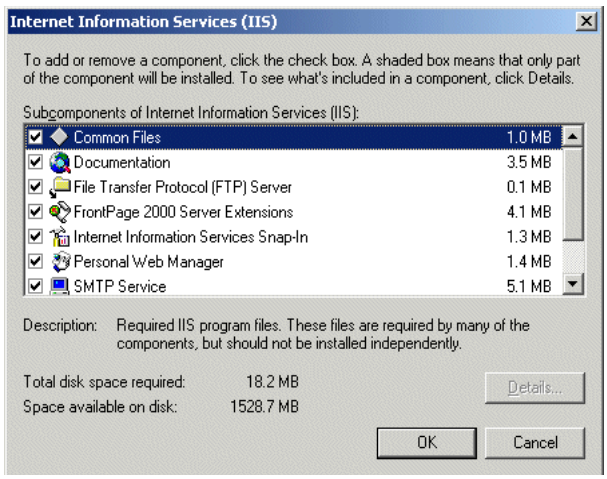
Internet Information Services (IIS)
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Internet Information Services (IIS):
Common Files 1.0 MB
Documentation 3.5 MB
File Transfer Protocol (FTP) Server 0.1 MB
FrontPage 2000 Server Extensions 4.1 MB
Internet Information Services Snap-In 1.3 MB
Personal Web Manager 1.4 MB
SMTP Service 5.1 MB
Description: Required IIS program files. These files are required by many of the components, but should not be installed independently.
Total disk space required: 18.2 MB
Space available on disk: 1528.7 MB
Details...
OK
Cancel

Figure A-3 *Internet Information Services (IIS) Dialog Box*

4 Verify that **Common Files**, **File Transfer Protocol (FTP) Server** and **Internet Information Services Snap-In** are checked and click **OK**.

The **Windows Components Wizard** dialog box displays (Figure A-2).

5 Click **Next** to complete the IIS installation.

INSTALLING IIS 4 SUBCOMPONENTS (WINDOWS 2003)

This procedure describes how you install IIS 4 subcomponents on the Windows 2003 operating system.

To install IIS 4 subcomponents on Windows 2003

1. From the **Start** menu, select **Settings >Control Panel > Add/Remove Programs**.
2. Click **Add/Remove Windows Components**.

   The **Windows Components Wizard** dialog box (Figure A-4) displays.

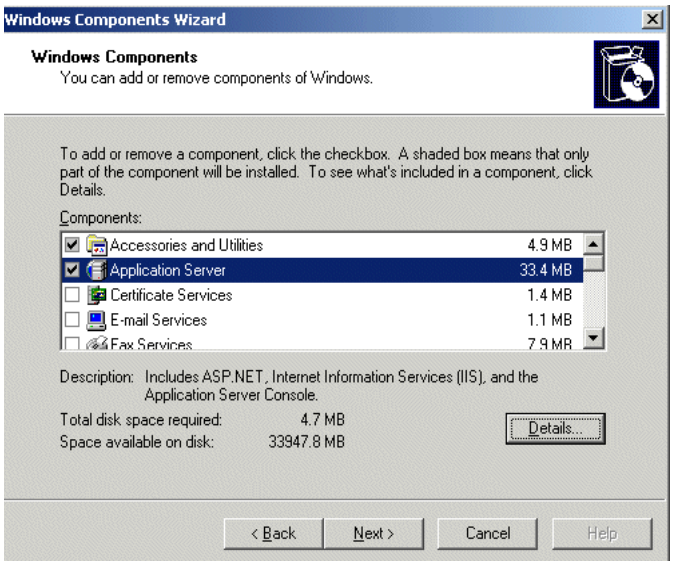
Windows Components Wizard
Windows Components
You can add or remove components of Windows.
To add or remove a component, click the checkbox. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Components:
Accessories and Utilities 4.9 MB
Application Server 33.4 MB
Certificate Services 1.4 MB
E-mail Services 1.1 MB
Fax Services 7.9 MB
Description: Includes ASP.NET, Internet Information Services (IIS), and the Application Server Console.
Total disk space required: 4.7 MB
Space available on disk: 33947.8 MB
Details...
< Back
Next >
Cancel
Help

Figure A-4 *Windows Components Wizard Dialog Box*

3. Select **Application Server** and click **Details**.

   The **Application Server** dialog box displays.

4 Select **Internet Information Services (IIS)** and click **Details**.

The **Internet Information Services (IIS)** dialog box (Figure A-3) displays.

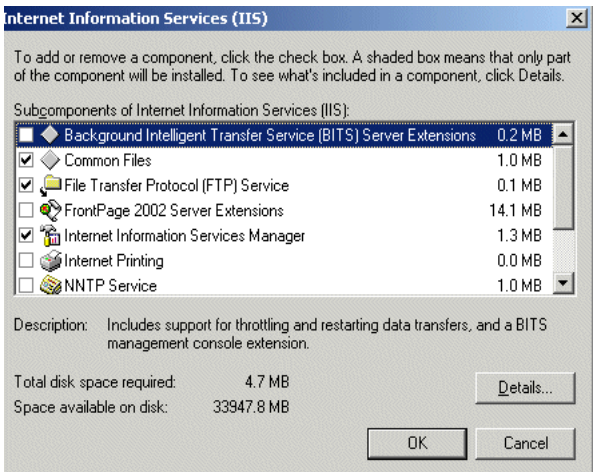
Internet Information Services (IIS)
To add or remove a component, click the check box. A shaded box means that only part of the component will be installed. To see what's included in a component, click Details.
Subcomponents of Internet Information Services (IIS):
Background Intelligent Transfer Service (BITS) Server Extensions 0.2 MB
Common Files 1.0 MB
File Transfer Protocol (FTP) Service 0.1 MB
FrontPage 2002 Server Extensions 14.1 MB
Internet Information Services Manager 1.3 MB
Internet Printing 0.0 MB
NNTP Service 1.0 MB
Description: Includes support for throttling and restarting data transfers, and a BITS management console extension.
Total disk space required: 4.7 MB
Space available on disk: 33947.8 MB
Details...
OK
Cancel

Figure A-5 *Internet Information Services (IIS) Dialog Box*

5 Verify that **Common Files**, **File Transfer Protocol (FTP) Server** and **Internet Information Services Manager** are checked and click **OK**.

The **Application Server** dialog box displays.

6 Click **OK**.

The **Windows Components Wizard** dialog box (Figure A-4) displays.

7 Click **Next** to complete the IIS installation.

CONFIGURING IIS 4 SUBCOMPONENTS (WINDOWS 2000/ 2003)

This section describes how you configure IIS 4 subcomponents on the Windows 2000 and 2003 operating systems, and how you set the LifeSize Gatekeeper default FTP path.

To configure IIS 4 subcomponents on Windows 2000 and 2003

1. Select **Start > Settings > Control Panel > Administrative Tools > Internet Services Manager**.

   The **Internet Information Services** panel (Figure A-6) displays.

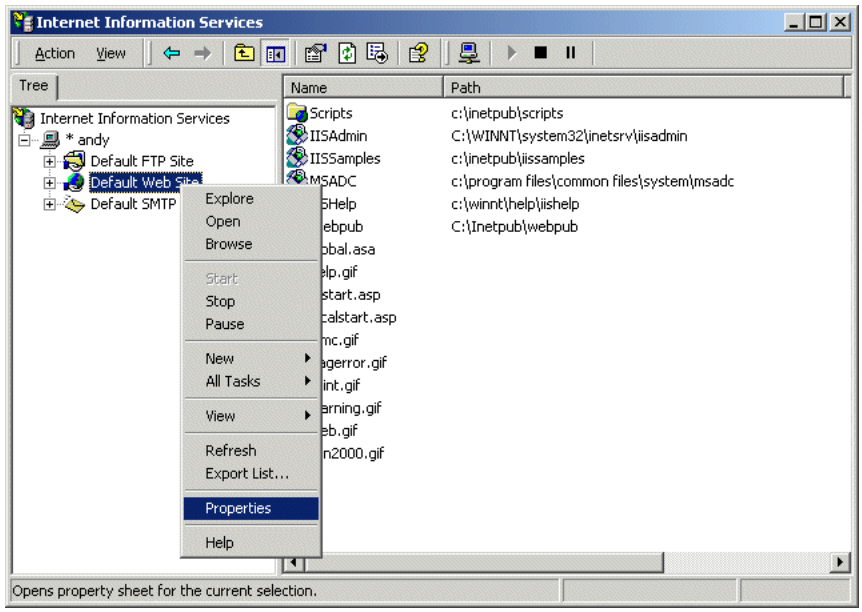

Figure A-6 *Internet Information Services Panel*

2. Click the local computer icon to display the tree structure.

3 Right click **Default Web Site** and select **Properties**, as shown in Figure A-6.

The **Default Web Site Properties** dialog box (Figure A-7) displays.

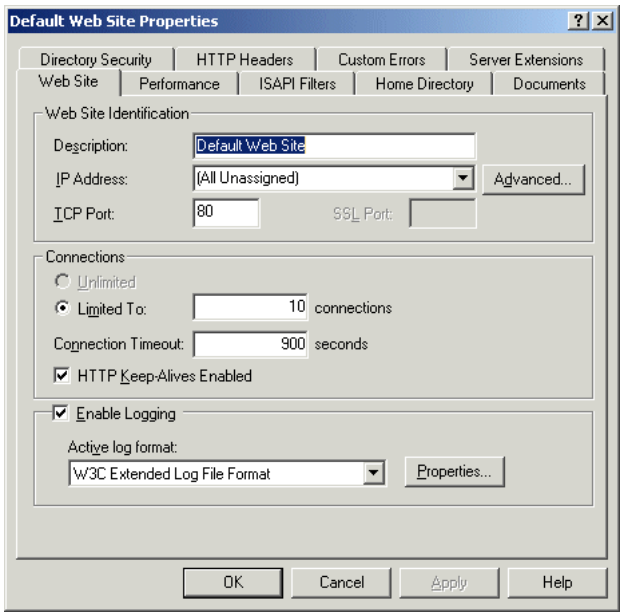

Figure A-7 *Default Web Site Properties Dialog Box*

4 Ensure that the **TCP Port** is not set to 80 and then click **OK**.

5 Click **OK** to close the Internet Services Manager.

6 Run the LifeSize Gatekeeper setup and set the LifeSize Gatekeeper log FTP default path.

Note LifeSize recommends that you set the **TCP Port** field to Port 10152.

To set the LifeSize Gatekeeper default FTP path

1. Select **Start > Programs > Administrative Tools > Internet Service Manager**.

   The **Internet Information Services** panel (Figure A-6) displays.
2. Expand the tree to view the **Default FTP Site** directory.
3. Right click **Default FTP Site** and select **New > Virtual Directory**, as shown in Figure A-8. The **New Virtual Directory Wizard** screen is displayed.

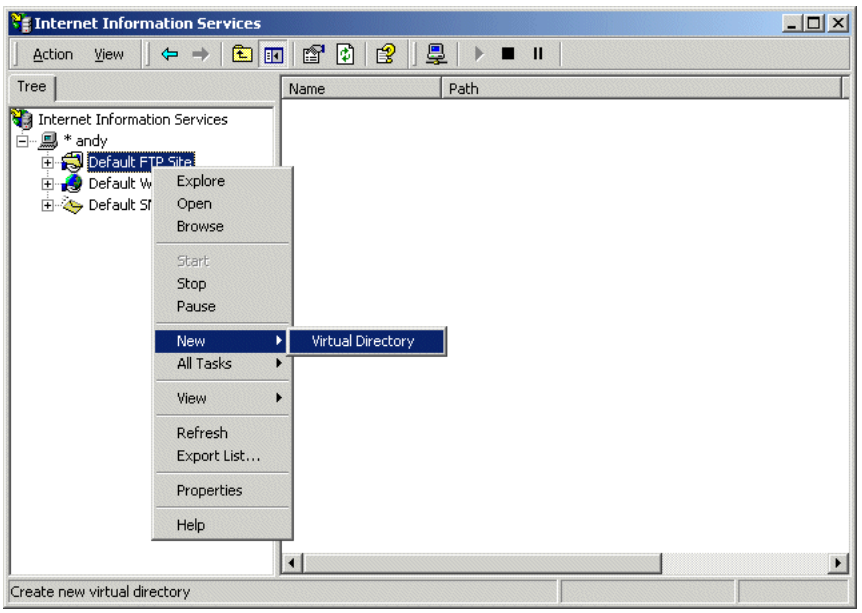

Figure A-8 *Internet Information Services Panel*

4. Type “gk_log” in the **Alias** text box, and click **Next**.
5. Navigate to the LifeSize Gatekeeper *logs* directory and select, and then click **Next**.
6. Check **Allow Read Access** and **Allow Write Access**, and then click **Finish**.

APPENDIX B

LIFESIZE GATEKEEPER CDR STRUCTURE

WHAT'S IN THIS APPENDIX

This appendix introduces you to the following:

- CDR Basics
- CDR Field Format
- Field Tags and Default Attributes
- Field Numeric Options
- Notes
- CDR Samples

CDR BASICS

The Call Detail Record (CDR) is a collection of H.323 call-related data such as alias address, call model and connection time. CDR data can be used as an input to a billing system or for accounting purposes. The CDR contains all call information in a text format. For example, the number 12 is stored as the string "12".

Data transmission between the CDR and the billing server is via TPKT over TCP/IP. The TPKT protocol inserts a header in front of all CDR messages. This header is four bytes long and contains three fields:

- ASCII character 3 (first byte)

  ASCII 3 represents an ETX (end of text) message.
- 0 (second byte)

- CDR message length (third and fourth bytes)

  The message length is calculated by multiplying the third byte by 256 and adding the value of the fourth byte. The resulting length includes the four bytes of the header itself.

Field Types

The CDR contains fixed length fields and variable length fields. The length of fixed length fields is predefined and is the same for all CDRs. For example, a field that represents the time and date will always have the same format and the same length since the string *02/05/2004:11:46:57* is 19 characters long.

Variable length fields (also called TLV— Tag, Length, Value) are fields where the length is unknown and can change from CDR to CDR. For example, the length of an alias field changes from alias to alias.

The CDR is formatted so that all fixed length fields appear first, enabling direct access to these fields from the beginning of the CDR according to their offset. All the variable length fields appear afterwards. Since the length of these fields is unknown, direct access to these fields is impossible and you should read this part of the CDR serially. Special tags are inserted in front of the variable length fields to help you identify the type of field and its length.

CDR Field Format

All fields start with a string that identifies them, followed by the "=" sign and then end with a new line ("\n"). For example, a fixed length field that contains the connection time will look like this:

```
Connect time=02/05/2004:11:46:57
```

However, there is a difference between the format of fixed length fields and variable length fields.

Fixed Length Fields

In fixed length fields, the field contains:

- A description string with the "=" sign.
- The value of the fixed length field.
- New line ("\n").

The length of the field is measured from the "=" sign to the end of the line.

Examples

```
Dest Call Signal Ip=172.020.001.082
Dest Call Signal Port=01131
```

```
Bandwidth=0000128000
```

If the field is shorter than the fixed length, zeros are inserted before the value of the field. This can be seen in both the *Dest Call Signal Port* field and the *Bandwidth* field above.

VARIABLE LENGTH FIELDS

The TLV (Tag, Length, Value) mechanism is used for variable length fields since these fields have different lengths. A variable length field contains:

- A description string with the "=" sign.
- Two characters representing the field tag in text format. The tag is a number that identifies the field.
- Three optional characters which give additional information about the field. For example, if the field is an alias, the alias type is stored in the first character. If the alias type is a party number, the party number type is stored in the next two characters. For more information on party number, see Adding or Modifying an Endpoint Alias on page 134.
- Three characters, representing the length of the field.
- The value of a field of variable length.
- New line ("\n").

Example 1

A source E.164 alias with a length of 5 and value 77777:

4	7	1	0	0	5	7	7	7	7	7

- 47 is the tag for source aliases.
- 1 identifies an E.164 alias.
- 005 is the alias length.
- 77777 is the alias value.

Example 2

A destination Party Number alias of Public Unknown type and value 1234:

4	8	6	0	1	0	0	4	1	2	3	4

- 48 is the tag for source aliases.
- 6 identifies a Party Number alias.

- 01 identifies Public Unknown.
- 004 is the alias length.
- 1234 is the alias value.

Field Tags and Default Attributes

Table B-1 shows the default format of the CDR. It contains all fields and their default attributes.

Note If a field is a variable length field by default, TLV appears in the *Default Length (chars)* column.

Table B-1 *CDR Fields and Default Attributes*

Tag	Identifying String	Default Length (chars)	Description
0	CDR Version Number	11	The version of the CDR generator. For example, 01.00.00.00.
1	Generator Type	1	The type of entity that generated this CDR. In this case, it will always be a gatekeeper. The options for this field are numeric and appear in Table B-9.
2	Record Type	1	Indicates whether a call has connected successfully. The options for this field are numeric and appear in Table B-10.
3	Generator Ras Ip	15	The RAS IP address of the CDR generator. Format: XXX.XXX.XXX.XXX.
4	Generator Ras Port	5	The RAS port of the CDR generator.
5	Generator Call Signal Ip	15	The Call Signaling IP address of the CDR generator. Format: XXX.XXX.XXX.XXX.
6	Generator Call Signal Port	5	The Call Signaling IP port of the CDR generator.
7	Generator Identifier	50	The CDR generator identifier.
8	Generation Time	17	The time at which the CDR was generated (GMT). Format: dd/mm/yyyy:hh:mm:ss.

Tag	Identifying String	Default Length (chars)	Description
9	Source Call Identifier	32	The call identifier of the incoming call (in hexadecimal converted to text).
10	Dest Call Identifier	32	The call identifier of the outgoing call (in hexadecimal converted to text).
11	Conference Id	32	The identifier of the conference to which this call belongs (in hexadecimal converted to text).
12	Call Model	1	Indicates whether a call is direct, routed or H.245 routed. The options for this field are numeric and appear in Table B-4.
13	Dest Zone	1	Indicates whether or not the destination of the call is in this gatekeeper zone. The options for this field are numeric and appear in Table B-6.
14	Source Endpoint Type	1	The source endpoint type. The options for this field are numeric and appear in Table B-5.
15	Source Call Signal Ip	15	The Call Signaling IP of the source endpoint. Format: XXX.XXX.XXX.XXX.
16	Source Call Signal Port	5	The Call Signaling port of the source endpoint.
17	Dest Endpoint Type	1	The destination endpoint type. The options for this field are numeric and appear in Table B-5.
18	Dest Call Signal Ip	15	The Call Signaling IP of the destination endpoint. Format: XXX.XXX.XXX.XXX.
19	Dest Call Signal Port	5	The Call Signaling port of the destination endpoint.
20	Bandwidth	10	The total bandwidth of the call in Kbps units.
21	Call Is To Service	1	Indicates whether or not the call is to a service.
22	ACF Time	19	The time at which the first ACF is sent (GMT). Format: dd/mm/yyyy:hh:mm:ss.

Tag	Identifying String	Default Length (chars)	Description
23	Connect time	19	The time at which the Connect message is sent to the source endpoint. For a direct call, connection time is zero (GMT). Format: dd/mm/yyyy:hh:mm:ss.
24	Release time	19	The time at which the Release Complete message is sent from the gatekeeper or received by the gatekeeper for a one-leg call. For a direct call, release time is zero (GMT). Format: dd/mm/yyyy:hh:mm:ss.
25	DRQ Time	19	The time at which the first DRQ message is received by the gatekeeper (GMT). Format: dd/mm/yyyy:hh:mm:ss.
26	Ring Time	5	The length of time (in milliseconds) that the call rings at the destination endpoint before a connection is made. This is the time between Alert and Connect (0 if Alert is not sent, or for a direct call).
27	Establishment Time	5	The length of time (in milliseconds) between the time at which the source endpoint receives an ACF message and the time at which the source endpoint receives a Connect message (0 for direct calls).
28	Source ARJ Reason	2	The reason for sending an ARJ message to the source endpoint. The options for this field are numeric and appear in Table B-7.
29	Dest ARJ Reason	2	The reason for sending an ARJ message to the destination endpoint. The options for this field are numeric and appear in Table B-7.
30	Source Release Cause	3	The *Cause* field from the Release Complete message which the source endpoint sends and receives (0 for a direct call).
31	Dest Release Cause	3	The *Cause* field from the Release Complete message which the destination endpoint sends and receives (0 for a direct call).
32	Source Release Reason	2	The *Reason* field from the Release Complete message which the source endpoint sends and receives (0 for a direct call). The options for this field are numeric and appear in Table B-8.

Tag	Identifying String	Default Length (chars)	Description
33	Dest Release Reason	2	The *Reason* field from the Release Complete message which the destination endpoint sends and receives (0 for a direct call). The options for this field are numeric and appear in Table B-8.
34	H450 Transfer Ended Call	1	A Boolean field indicating that a call has ended because one of the parties was transferred to another destination.
35	H450 Transferred To Signal IP	15	The IP address of the leg to which the call is transferred.
36	H450 Transferred To Signal Port	5	The port of the leg to which the call is transferred.
37	H450 Transfer Started Call	1	A Boolean field indicating that this is a call that began from a transfer operation.
38	H450 Transferred From Signal IP	15	The Call Signaling IP address of the transferring party of the call.
39	H450 Transferred From Signal Port	5	The Call Signaling port of the transferring party of the call.
40	H450 Transferred From Call Id	32	The call identifier of the party that transfers the call and then leaves the call. In hexadecimal converted to text.
41	H450 Call Record Type	1	For the H.450.3 Forwarding Supplementary Service. This field indicates whether the purpose of the call is activation, deactivation or check restriction. The options for this field are numeric and appear in Table B-12.
42	H450 Forwarded Call	1	A Boolean field indicating that a call was forwarded from its original destination.
43	H450 Forward Type	1	Indicates the type of forwarding: CFB, CFNR or CFU. The field options are numeric and appear in Table B-11.
44	H450 Forwarded From Signal IP	15	The Call Signaling IP of the original destination of the call.
45	H450 Forwarded From Signal Port	5	The Call Signaling port of the original destination of the call.
46	H450 Forwarded From Alias	TLV	The first alias of the original destination of the call.

Tag	Identifying String	Default Length (chars)	Description
47	H450 Transferred From Alias	TLV	Indicates the alias of the transferring leg of an original call in cases where an existing call passes to a new destination endpoint and the original source endpoint drops out of the call.
48	Source Alias	TLV	The source aliases of the call.
49	Dest Alias	TLV	The destination alias used to connect a call. This destination alias is used to perform the actual address resolution. This destination alias may be different from the destination alias used by the endpoint to place the call, since forwarding may be part of the destination resolution.
50	Destination Extra	TLV	An extra destination for video calls with several B channels.
51	Remote Extension	TLV	Remote extension (contains the alias address of a called endpoint in cases where the call crosses multiple gateways).
52	Service Number	TLV	The service prefix number.
53	Calling Party Number	TLV	The Fixed Calling Party Number of the call.
54	Call Initiator Type	1	Indicates the call initiator (1 = a terminal, 4 = the LifeSize Gatekeeper).
55	Call Media Type Video	1	0 = the call does not use this media type, 1 = the call does use this media type. Missing from the CDR when the LifeSize Gatekeeper is in Direct Mode.
56	Call Media Type Audio	1	0 = the call does not use this media type, 1 = the call does use this media type. Missing from the CDR when the LifeSize Gatekeeper is in Direct Mode.
57	Call Media Type Data	1	0 = the call does not use this media type, 1 = the call does use this media type. Missing from the CDR when the LifeSize Gatekeeper is in Direct Mode.
58	Call Is From Service	1	Indicates whether or not the call is from a service.
59	From Service Number	TLV	The number identifying the service.

Tag	Identifying String	Default Length (chars)	Description
60	Conference Number	TLV	The conference identifier when the LifeSize Multipoint invites a participant.
61	Is Fall Back Call	1	Indicates whether or not the call is a fallback call.
62	Orig Dest Alias	TLV	The original call alias before fallback.
63	Source Zone	1	Indicates whether or not the source of the call is in this gatekeeper zone. The options for this field are numeric and appear in Table B-6.
64	Real Connect Time	19	Indicates the actual time at which a LAN-to-ISDN call connects to the ISDN terminal. Where a gateway does not support this field, the value in the *Real Connect Time* field is the same as the value in the *Connect time* field (tag 23).

Field Numeric Options

Alias Tags

Table B-2 Alias Tags

Tag	Alias Type
1	E.164
2	H.323ID
3	URL ID
4	Transport ID
5	E-mail ID
6	Party Number

Party Number Tags

Table B-3 Party Number Tags

Tag	Party Number Type
1	Public Unknown
2	Public International Number
3	Public National Number
4	Public Network Specific Number
5	Public Subscriber Number
6	Public Abbreviated Number
7	Data Party Number
8	Telex Party Number
9	Private Unknown
10	Private Level 2 Regional Number
11	Private Level 1 Regional Number

Tag	Party Number Type
12	Private PISN Specific Number
13	Private Local Number
14	Private Abbreviated Number
15	National Standard Party Number

Call Model Tags

Table B-4 Call Model Tags

Tag	Call Model
0	Undefined
1	Direct
2	Gatekeeper Routed
3	H.245 Routed

Endpoint Type Tags

Table B-5 Endpoint Type Tags

Tag	Endpoint Type
0	Undefined
1	Terminal
2	Gateway
3	MCU
4	Gatekeeper

Destination Zone

Table B-6 Destination Zone Tags

Tag	Destination Zone	Description
0	Undefined	The destination zone is not defined.
1	External	The call is to an out-of-zone endpoint.
2	Local	The call is to an in-zone endpoint.

ARJ Reason Tags

Table B-7 ARJ Reason Tags

Tag	ARJ Reason
0	Undefined
1	Called Party Not Registered
2	Invalid Permission
3	Request Denied
4	Caller Not Registered
5	Route Call To GK
6	Invalid Endpoint Identifier
7	Resource Unavailable
8	Security Denial
9	QoS Control Not Supported
10	Incomplete Address

Release Reason Tags

Table B-8 Release Reason Tags

Tag	Release Reason
0	Undefined
1	No Bandwidth

Tag	Release Reason
2	Gatekeeper Resources
3	Unreachable Destination
4	Destination Rejection
5	Invalid Revision
6	No Permission
7	Unreachable Gatekeeper
8	Gateway Resources
9	Bad Format Address
10	Adaptive Busy
11	In Conference
12	Facility Call Deflection
13	Security Denied
14	Called Party Not Registered
15	Caller Not Registered
16	Forced Drop
17	Normal Drop

GENERATOR TAGS

Table B-9 Generator Type Tags

Tag	Generator Type
0	Undefined
1	Gatekeeper
2	Gateway

RECORD TYPE TAGS

Table B-10 Record Type Tags

Tag	Record Type	Description
0	Undefined	The record type is not defined.
1	Successful Call	For Routed Mode: the call was connected. For Direct Mode: no ARJ was sent.
2	Unsuccessful Call	For Routed Mode: the call was not connected or ARJ was sent to one of the endpoints. For Direct Mode: ARJ was sent to one of the endpoints.

H.450 FORWARD TYPE TAGS

Table B-11 H.450 Forward Type Tags

Tag	H.450 Forward Type	Description
0	Undefined	The H.450 Forward Type is not defined.
1	CFU	Unconditional forward.
2	CFB	Forward on busy.
3	CFNR	Forward on no response.
4	CNFREG	Forward when not registered.

H.450 CALL RECORD TYPE TAGS

Table B-12 H.450 Call Record Type Tags

Tag	H.450 Call Record Type	Description
0	Undefined	The H.450 Call Record Type is not defined.
1	Activation	The call is activated.
2	Deactivation	The call is deactivated.
3	Check Restriction	The call is check restricted.

NOTES

- If a fixed length field is unavailable, such as the connection time in a direct call, zero is inserted as the value of that field. The default format of the field does not change. For example:

  H.450 Transferred To Signal IP = 000.000.000.000

  ```
  H.450 Transferred From Call Id =
  00000000000000000000000000000000
  ```

- If a variable length field is unavailable, such as the *Destination Extra* field which is not always used, this field will not be part of the CDR.
- CDR media fields are available only when the LifeSize Gatekeeper operates in H.245 Routed mode.

CDR SAMPLES

CDR FOR A STANDARD CALL

E.164 alias “111” calls E.164 alias “20” using video, audio and data media.

```
CDR Version Number=00.00.00.03
Generator Type=1
Record Type=1
Generator Ras Ip=172.020.069.190
Generator Ras Port=01719
Generator Call Signal Ip=172.020.069.190
Generator Call Signal Port=01720
Generator Identifier=GK
Generation Time=27/05/2004:13:50:47
Source Call Identifier=0217b18782e76b2237215634343434ef
Dest Call Identifier=0217b18782e76b2237215634343434ef
Conference Id=0217b18782e76b2237225634343434ef
Call Model=3
Dest Zone=0
Source Endpoint Type=1
Source Call Signal Ip=172.020.069.190
Source Call Signal Port=01294
Dest Endpoint Type=1
Dest Call Signal Ip=172.020.069.190
Dest Call Signal Port=01413
Bandwidth=0000256000
Call Is To Service=0
ACF Time=27/05/2004:13:50:35
Connect time=27/05/2004:13:50:35
Release time=27/05/2004:13:50:47
DRQ Time=27/05/2004:13:50:47
Ring Time=00090
Establishment Time=00280
Source ARJ Reason=00
Dest ARJ Reason=00
Source Release Cause=0-1
Dest Release Cause=0-1
```

```
Source Release Reason=00
Dest Release Reason=00
H450 Transfer Ended Call=0
H450 Transferred To Signal IP=000.000.000.000
H450 Transferred To Signal Port=00000
H450 Transfer Started Call=0
H450 Transferred From Signal IP=000.000.000.000
H450 Transferred From Signal Port=00000
H450 Transferred From Call
Id=00000000000000000000000000000000
H450 Call Record Type=0
H450 Forwarded Call=0
H450 Forward Type=0
H450 Forwarded From Signal IP=000.000.000.000
H450 Forwarded From Signal Port=00000
Source Alias=481003111
Dest Alias=49100220
Calling Party Number=531003111
Call Initiator Type=1
Call Media Type Video=1
Call Media Type Audio=1
Call Media Type Data=1
Call Is From Service=0
Conference Number=6000588028
Is Fall Back Call=0
Source Zone=2
Real Connect time=27/05/2004:13:50:35
```

CDR FOR A FORWARDED CALL

E.164 alias “111” calls E.164 alias “20” via a gateway. The gateway forwards the call unconditionally.

```
CDR Version Number=00.00.00.03
Generator Type=1
Record Type=1
Generator Ras Ip=172.020.069.190
Generator Ras Port=01719
Generator Call Signal Ip=172.020.069.190
```

```
Generator Call Signal Port=01720
Generator Identifier=GK
Generation Time=27/05/2004:14:09:32
Source Call Identifier=0217b18ec10a989937225634343434ef
Dest Call Identifier=0217b18ec16ced111e2d5634343434ef
Conference Id=0217b18ec10a989937235634343434ef
Call Model=3
Dest Zone=0
Source Endpoint Type=1
Source Call Signal Ip=172.020.069.190
Source Call Signal Port=01294
Dest Endpoint Type=1
Dest Call Signal Ip=172.020.069.190
Dest Call Signal Port=01413
Bandwidth=0000256000
Call Is To Service=0
ACF Time=27/05/2004:14:09:07
Connect time=27/05/2004:14:09:07
Release time=27/05/2004:14:09:32
DRQ Time=27/05/2004:14:09:32
Ring Time=00090
Establishment Time=00281
Source ARJ Reason=00
Dest ARJ Reason=00
Source Release Cause=0-1
Dest Release Cause=0-1
Source Release Reason=08
Dest Release Reason=08
H450 Transfer Ended Call=0
H450 Transferred To Signal IP=000.000.000.000
H450 Transferred To Signal Port=00000
H450 Transfer Started Call=0
H450 Transferred From Signal IP=000.000.000.000
H450 Transferred From Signal Port=00000
H450 Transferred From Call
```

```
Id=00000000000000000000000000000000
H450 Call Record Type=0
H450 Forwarded Call=1
H450 Forward Type=1
H450 Forwarded From Signal IP=172.020.069.183
H450 Forwarded From Signal Port=01210
H450 Forwarded From Alias=461003108
Source Alias=481003111
Dest Alias=49100220
Calling Party Number=531003111
Call Initiator Type=1
Call Media Type Video=1
Call Media Type Audio=1
Call Media Type Data=1
Call Is From Service=0
Conference Number=6000588028
Is Fall Back Call=0
Source Zone=2
Real Connect time=27/05/2004:14:09:07
```

CDR FOR A CALL TO A SERVICE

E.164 alias “106” calls E.164 alias “1234” using service 99 via a LifeSize Gatekeeper.

```
CDR Version Number=00.00.00.03
Generator Type=1
Record Type=1
Generator Ras Ip=172.020.001.234
Generator Ras Port=01719
Generator Call Signal Ip=172.020.001.234
Generator Call Signal Port=01720
Generator Identifier=GK
Generation Time=28/05/2004:07:05:02
Source Call Identifier=0217b31b2bbbc33b18245634343434ef
Dest Call Identifier=0217b31b2bbbc33b18245634343434ef
Conference Id=0217b31b2bbbc33b18255634343434ef
Call Model=3
Dest Zone=0
```

```
Source Endpoint Type=1
Source Call Signal Ip=172.020.001.234
Source Call Signal Port=02939
Dest Endpoint Type=2
Dest Call Signal Ip=172.020.001.234
Dest Call Signal Port=05070
Bandwidth=0000512000
Call Is To Service=1
ACF Time=28/05/2004:07:03:56
Connect time=28/05/2004:07:04:00
Release time=28/05/2004:07:05:01
DRQ Time=28/05/2004:07:05:01
Ring Time=04375
Establishment Time=05176
Source ARJ Reason=00
Dest ARJ Reason=00
Source Release Cause=0-1
Dest Release Cause=0-1
Source Release Reason=02
Dest Release Reason=02
H450 Transfer Ended Call=0
H450 Transferred To Signal IP=000.000.000.000
H450 Transferred To Signal Port=00000
H450 Transfer Started Call=0
H450 Transferred From Signal IP=000.000.000.000
H450 Transferred From Signal Port=00000
H450 Transferred From Call
Id=00000000000000000000000000000000
H450 Call Record Type=0
H450 Forwarded Call=0
H450 Forward Type=0
H450 Forwarded From Signal IP=000.000.000.000
H450 Forwarded From Signal Port=00000
Source Alias=481003106
Source Alias=484021172.020.055.015:01112
```

```
Source Alias=485013106@company.com
Dest Alias=491006991234
Service Number=5200299
Calling Party Number=531003106
Call Initiator Type=1
Call Media Type Video=1
Call Media Type Audio=1
Call Media Type Data=1
Call Is From Service=0
Conference Number=6000588028
Is Fall Back Call=0
Source Zone=2
Real Connect time=28/05/2004:07:04:05
```

APPENDIX C

LIFESIZE GATEKEEPER GROUP HUNTING

WHAT'S IN THIS APPENDIX

This appendix describes how to configure the LifeSize Gatekeeper Group Hunting feature and includes the following:

- Overview
- Before You Begin
- Configuring Group Hunting

OVERVIEW

Group Hunting enables the LifeSize Gatekeeper to perform load balancing for a group of endpoints. To achieve this, you define an alias for several H.323 endpoints thereby grouping them together. A group alias can be the existing online alias of one of the members of the group, or you can configure a new predefined alias for all the endpoints in the group.

BEFORE YOU BEGIN

Before you configure Group Hunting, note the following:

- You can configure Group Hunting with or without checking the **Merge predefined and online aliases upon registration** option in the **Basics** section of the **Settings** tab.
  - If you configure Group Hunting with the **Merge predefined and online aliases upon registration** option, you must define the new alias as a service before you define the Group Hunting.
  - If you configure Group Hunting without the **Merge predefined and online aliases upon registration** option, you can define the new alias and the Group Hunting in any order.

CONFIGURING GROUP HUNTING

This procedure describes how you configure the LifeSize Gatekeeper Group Hunting feature.

To configure an alias for Group Hunting

1. Check the **Merge predefined and online aliases upon registration** option in the **Basics** section of the **Settings** tab.
2. Define the new alias as a service in the **Service Properties** dialog box in the **Services** tab.
3. Uncheck the **Conference hunting** option in the **Service Properties** dialog box in the **Services** tab.
4. In the **Endpoints** section of the **Endpoints** tab, double click the relevant online endpoint, or select the endpoint and click **Properties**.

   The **Online Endpoint Properties** dialog box displays.
5. Click **Make Predefined**.

   The **Predefined Endpoint Properties** dialog box displays.
6. Click **Add** and type the new alias in the **Add Alias** dialog box.
7. Click **OK** in the **Add Alias** dialog box, and then click **Upload** in the **Predefined Endpoint Properties** dialog box.

Note Group Hunting cannot work when the **Conference hunting** option is checked in the **Service Properties** dialog box in the **Services** tab.

APPENDIX D

LIFESIZE GATEKEEPER DIAL PLAN VERSION 2

WHAT'S IN THIS APPENDIX

This appendix describes the LifeSize Gatekeeper Dial Plan and includes the following:

- Introduction to the Dial Plan.
- Network criteria that affect the design of a dial plan.
- Configuration tools for customizing a dial plan to suit your organizational requirements.

OVERVIEW

In traditional telephony systems, a dial plan is a front-end system that allows users to call each other by dialing a number on a telephone. In voice and video conferencing over IP, a dial plan is a system that allows participants in point-to-point or multipoint conferences to call each other or join conferences. Participants type or dial a string of digits or characters at their terminal or IP phone.

The LifeSize Gatekeeper Dial Plan provides "configuration tools" which allow network administrators to build an IP dial plan that suits the requirements of their organization and network. These tools enable you to:

- Configure gatekeepers in a flat and/or hierarchical topology to enable efficient location of called endpoints.
- Assign extension numbers or aliases to endpoints.
- Configure gateways, LifeSize Multipoints and gatekeepers to support services.
- Assign prefixes to facilitate dialing within and between zones in the IP network, and dialing to and from PSTN networks.

The LifeSize Gatekeeper, LifeSize Multipoint and LifeSize Gateway support the LifeSize Gatekeeper Dial Plan and work in a unified way to create an integrated dial plan. The LifeSize Gatekeeper is at the heart of the dial plan.

The LifeSize Gatekeeper Dial Plan is scalable. Because it allows a hierarchical architecture, you can start a network with a single zone (one gatekeeper) and a small number of endpoints and scale up the dial plan as the network grows.

The LifeSize Gatekeeper Dial Plan is suitable for both Service Provider and enterprise requirements. The hierarchical architecture facilitates the setting up of enterprise networks, large Service Provider deployments and dialing structures that support national and international dialing.

Understanding Your Network

There are a number of criteria that you should consider before defining a dial plan. These include network size, whether dialing is internal or external or both, scalability, whether you want PSTN numbering or alias numbering, and whether you wish to create a PBX-like environment. A further consideration is the relative positioning of gatekeepers within the network.

What Kind of Network Do You Have?

The kind of network you have will determine the kind of LifeSize Gatekeeper Dial Plan you will build. The following criteria will help you understand what kind of network you have:

- **Network Scale**

  Network scale is a key factor when deciding about the type of LifeSize Gatekeeper Dial Plan you will build. If the network is large, setting up and configuring a hierarchy of gatekeepers is recommended. If the network is small, a simple, flat topology may be sufficient.

- **Network Usage**

  The way your network will be used will affect the dial plan. If the network will be used for internal as well as external calls, the LifeSize Gatekeeper Dial Plan should include a way to dial out from the inside network to the outside network. If the network will be used for internal calls only, aliases or simple four- or five-digit numbers may be preferable to longer PSTN-like numbers.

- **Expected Network Growth**

  Scalability is an important issue. Setting up and configuring devices in the network is time-consuming. When a network grows and new endpoints, dialing areas and gatekeepers are added there may be a need to renumber the entire system. It is recommended to plan for growth when designing the dial pan.

- **Network Device Population**

  Network population affects the dial plan. It is worthwhile verifying what devices populate the network. Are there only terminals? Are there other devices such as gateways and LifeSize Multipoints? How many gatekeepers do you require?

- **Network Organization**

  If there are gatekeepers and gateways, check whether they are in the same NOC. Find where POPs are located and where they are dispersed through the network. It is useful to place a LifeSize Gatekeeper at each POP.

- **Services that the Network Provides**

  Services are a key factor in the LifeSize Gatekeeper Dial Plan. Analyze the types of services your network provides.

  Services can be local to a zone or they can be global. They can be centralized or decentralized. A service can be a gateway to one or many PSTN lines.

- **Types of Gatekeepers**

  It is important to understand the types of gatekeepers in the network. Are there only LifeSize Gatekeeper installations or is there a mixture of LifeSize Gatekeeper and non-LifeSize gatekeepers?

GATEKEEPER TOPOLOGY

If you have more than one gatekeeper in the network, the way the gatekeepers are arranged in your network may affect the LifeSize Gatekeeper Dial Plan.

The criteria discussed in the previous section will help to determine the gatekeeper topology that best suits your requirements. You can arrange gatekeepers in a hierarchical or flat topology or a mixture of both.

FLAT TOPOLOGY (NEIGHBOR GATEKEEPERS)

A flat topology is created through the use of Neighbor Gatekeepers. In a small network or in a grouped part of the network, Neighbor Gatekeepers facilitate the quick location of destination endpoints.

EXAMPLE

1. Endpoint A is registered to LifeSize Gatekeeper A. LifeSize Gatekeeper A has been configured with Neighbor Gatekeeper.
2. Endpoint A dials to endpoint B.
3. LifeSize Gatekeeper A searches its directory to see if endpoint B is in its zone.
4. If it is not LifeSize Gatekeeper A sends an LRQ (Location Request) to one of its Neighbor Gatekeepers in an attempt to connect the call to endpoint B.

This method provides a fast and efficient way of locating endpoints.

A Neighbor Gatekeeper topology is suitable for a limited number of gatekeepers. If there are too many gatekeepers, then maintenance may be cumbersome. Each time a new gatekeeper "joins" the network each existing gatekeeper's Neighbor Gatekeeper list must be manually updated to include the new gatekeeper.

Note For more information about Neighbor Gatekeepers, see the Neighbors Tab chapter and the Hierarchy Tab chapter.

HIERARCHICAL TOPOLOGY

A hierarchical topology consists of parent and child gatekeepers. The network can be regarded as a collection of groups of parents and children. Each gatekeeper knows its children, its parent and optionally, its neighbors.

Hierarchies are suitable for large networks and lend themselves to growth without requiring additional configuration of existing gatekeepers. When the network grows, all you need to do is add a new parent or child to the existing network.

In hierarchical topologies, endpoints typically register with the lowest-level gatekeeper (leaf). Exceptions to this generalization include endpoints that provide call-center services or endpoints that are gateways.

Note For more information about hierarchies, see the Hierarchy Tab chapter.

Mixed Topology

In larger networks, it usually makes sense to apply a mixed topology of neighbors and hierarchies. Neighbor Gatekeepers are useful when there is frequent inter-zone dialing. One or more gatekeepers can be grouped as Neighbor Gatekeepers within adjacent zones.

With Neighbor Gatekeepers, location of the destination endpoint and call routing are quicker than when LRQs are multicast or sent “upwards” in the hierarchy.

Note If one or more LifeSize Gatekeeper instances have the same parent, it does not necessarily imply that they are neighbors. A Neighbor Gatekeeper needs to be explicitly defined.

Criteria For Deciding The Type of Topology

The following guidelines may help you decide what type of topology best suits your network:

- Define the topology so that you don’t need to change numbers even when the network scales.
- If your network is small and you don’t anticipate much growth, use a Neighbor Gatekeeper and not a hierarchical topology.
- In a hierarchical topology, if endpoints in one zone dial frequently to endpoints in another zone define their gatekeepers as Neighbor Gatekeepers

Numbering

The next step in designing your dial plan is to decide on the type of numbering system you wish to apply. Some networks require dialing by means of aliases and others need to support PSTN numbering. When allocating numbers another factor to consider is the length or number of digits in the endpoint extension number.

You allocate endpoint numbers in the LifeSize Gatekeeper by assigning aliases. An alias can be a phone number, URL address, transport address (IP address:port), name, e-mail address or party number.

Note For more information about assigning numbers to endpoints, see the Endpoints Tab chapter.

PSTN-Like Numbering

The LifeSize Gatekeeper Dial Plan has been designed so that users can dial PSTN (E.164) numbers. This means that when a user dials a number to request a service and/or to call another phone or terminal, the user does not need to be aware of the location of the dialed number. It is irrelevant whether the destination number is in an IP or PSTN network.

The advantages of endpoints registering with a LifeSize Gatekeeper with a full PSTN-like number are:

- Endpoints in an organization support PSTN-like dialing.
- In an enterprise that uses an accounting system a PSTN-like number is useful for mixing internal accounting with PSTN billing.
- Service Provider billing is simplified as end-users can be clearly identified. Full numbers also facilitate integration of billing for different types of communication.

Aliases That Are Not Numbers

PSTN numbering may not be necessary or suitable for all environments. There are certain environments that may prefer a dial plan that uses URL or e-mail aliases instead of numbers. These types of environments are usually closed organizations or enterprises where there is no dialing out to PSTN.

Note If you prefer to use aliases instead of PSTN-like numbering then LifeSize recommends using version 1 of the Dial Plan. For more information about selecting version 1 of the Dial Plan, see Basics on page 46.

Number of Digits

The decision about the number of digits in the endpoint extension should take the current and future scale of your network into account.

If the network is small and there are currently less than 1000 endpoints, and you don't anticipate growth beyond 1000 endpoints, it is quite acceptable to give each endpoint a three-digit number. When the network grows beyond 1000 endpoints, you have to change all the numbers to four- or five-digit numbers, or you can establish new zones with endpoints registered with different gatekeepers.

Prefixes

Prefixes are characters or digits that are added to the dial strings to:

- Request a service.
- Provide zone information.
- Request out-of-zone dialing.

SERVICES

You request a service by dialing a prefix. The way the LifeSize Gatekeeper Dial Plan handles the request depends on the type of service. There are two types of services—global and local.

Note For more information about services, see the Services Tab chapter.

GLOBAL SERVICES

A global service is a service that is available to everyone using the network. It is identified by a universal prefix. For example, a gateway service for dialing out to the PSTN may be global with a universal prefix such as “9”. All entities in the network recognize that the prefix “9” indicates that the call should be routed to the PSTN via a gateway.

In this case, the dial string would be:

Global Service Prefix-[Zone Prefix]-endpoint number

such as:

9-1201-5294300

or *9-5294300*

Note For more information about global services, see the Services Tab chapter.

LOCAL SERVICES

A local service is local to a zone or to a part of the network. Its prefix may indicate different services in different parts of the network. For example, in one zone the service prefix for a video LifeSize Multipoint conference may be “80” while in another zone “80” might indicate a voice-only LifeSize Multipoint conference.

In this case, the dial string would be:

[Zone Prefix]-Local Service Prefix-endpoint number

such as:

1201-80-5645

or 80-5645

Note For more information about local services, see the Services Tab chapter.

Zone Prefixes

Endpoints that register to a gatekeeper are in a zone of that gatekeeper. You can define one or two zone prefixes for each LifeSize Gatekeeper.

Gatekeepers identify their neighbors by their zone prefixes. A LifeSize Gatekeeper that has been configured with Neighbor Gatekeepers maintains lists of the zone prefixes of all Neighbor Gatekeepers.

The zone prefix can be used in the same way as an area code in regular telephony. This means that you can configure the LifeSize Gatekeeper Dial Plan so that an endpoint dialing to another endpoint in the same zone needs only to dial the endpoint extension number without dialing the zone prefix.

However, you can also configure the LifeSize Gatekeeper Dial Plan so that even in the same zone endpoints should dial the entire number.

Note For more information about zone prefixes, see the Services Tab chapter.

Exit Zone Prefixes

Exit zone prefixes allow you to dial out of a zone. When a gatekeeper receives a dial string with an exit zone prefix, the gatekeeper handles the call as follows:

- If the LifeSize Gatekeeper has no exit zone prefix it attempts to locate numbers within its zone.
- If the LifeSize Gatekeeper has been configured with an exit zone prefix then when the LifeSize Gatekeeper recognizes an exit zone prefix in the dialed string, the LifeSize Gatekeeper routes the call out of the zone to a Neighbor Gatekeeper, parent or a child gatekeeper depending on the topology.

Note For more information about zone prefixes, see the Services Tab chapter.

Stripping

Stripping is a form of digit manipulation whereby a gatekeeper can be configured to strip (discard) certain digits from a dial string so that the dialed number will be recognized by the gatekeeper and routed to the right destination. Examples of stripping include:

- Exit zone stripping where the originating gatekeeper strips the exit zone prefix before routing the call.
- Self-zone stripping where the gatekeeper recognizes its own zone prefix and strips it before routing the call.

You can configure the LifeSize Gatekeeper to strip or not strip prefixes depending on the circumstances. For example, you can configure the same LifeSize Gatekeeper to strip (or not to strip) the zone prefix for IP network-to-IP network calls and to strip (or not strip) the zone prefix for IP-to-ISDN network calls.

Note For more information about stripping, see Dial Plan on page 57.

The following scenario demonstrates stripping:

In a national enterprise the topology of the network is hierarchical. The parent gatekeeper is located at Head Office. Each Branch Office has a gatekeeper registered as a child to the Head Office gatekeeper.

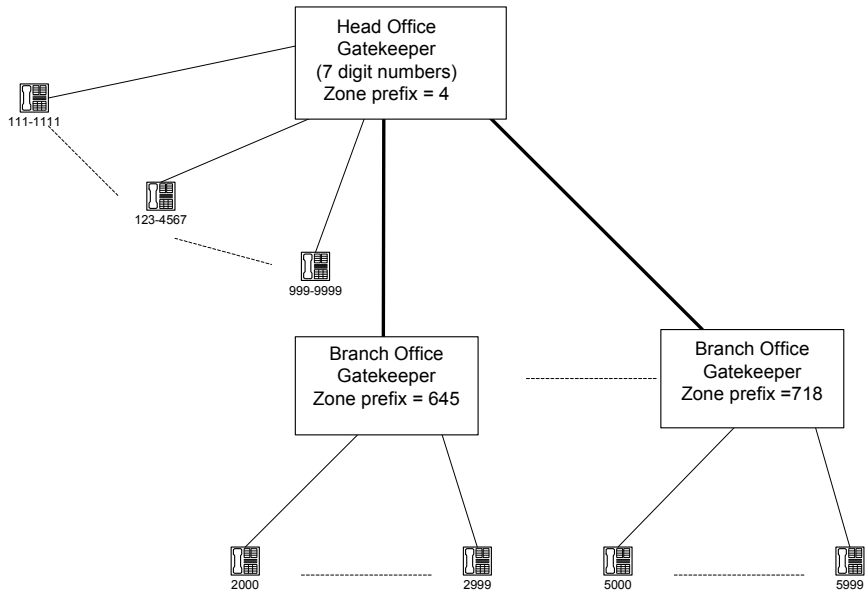

Figure D-1 *Stripping*

Branch Office Configuration

The gatekeeper in Branch Office 645 has been configured as follows:

- Endpoints have numbers that contain four digits.

- Endpoints are registered with the Branch Office gatekeeper.
- The zone prefixes of the Branch Office gatekeepers are three-digit numbers such as 645.
- When endpoints dial within a Branch Office they dial four digits.
- Calls dialing into a Branch Office need to dial the zone prefix followed by the extension number. For example, 645-2000.
- The Local Office gatekeepers have been configured to perform self-zone stripping.

Head Office Configuration

The Head Office gatekeeper has been configured as follows:

- Endpoints have numbers that contain seven digits.
- Endpoints are registered with the Head Office gatekeeper.
- The zone prefix of the Head Office gatekeeper is 4.

What Happens to Incoming Calls

1. An external endpoint dials 645-2000.
2. The Head Office gatekeeper routes the call to the gatekeeper in Branch Office 645.
3. The gatekeeper in Branch Office 645 strips 645 from the number and routes the call to endpoint 2000.

What Happens to Outgoing Calls

1. Endpoint 2000 dials 4-1234567.
2. The gatekeeper in Branch Office searches in its zone for the number 4-1234567.
   - If the search is unsuccessful, the gatekeeper searches for zone prefix 4 among its children and neighbors.
   - If the search is still unsuccessful, the gatekeeper routes the call to the Head Office gatekeeper. The Head Office gatekeeper strips the 4 (zone prefix) and routes the call to its endpoint 1234567.

PARENT FILTERS

One of the objectives of a well-defined LifeSize Gatekeeper Dial Plan is to locate endpoints efficiently. You can configure the LifeSize Gatekeeper to support parent filters. When the LifeSize Gatekeeper fails to resolve a destination address, the LifeSize Gatekeeper searches for the destination first among its children, then among its neighbors and then via its parent. Parent filters enable the LifeSize Gatekeeper to avoid unnecessary searches directed to the parent.

The LifeSize Gatekeeper sends an LRQ to the Parent Gatekeeper when the dialed number of the call matches one of the defined parent filters. The Parent Gatekeeper begins searching for the destination endpoint only when the dialed number matches the parent filter.

Note For more information about parent filters, see About Parent Filters on page 220.

The following example describes what happens when a LifeSize Gatekeeper has been configured with parent filters:

- Branch Office gatekeeper is the child of the Head Office gatekeeper.
- Endpoint A is registered to the Branch Office gatekeeper which has been configured with parent filters 4, 0.
- Endpoint B (645-1234567) is registered to the Head Office gatekeeper.
- A Service Provider gatekeeper with zone prefix 03 and the Head Office gatekeeper are neighbors.

SCENARIO 1

1. Endpoint A dials to 4-1234567.
2. The Branch Office gatekeeper would normally send LRQs first to the children, then to the neighbors, and then to the parent. Because one of the parent filters is 4 the Branch Office gatekeeper sends an LRQ to the Head Office gatekeeper.

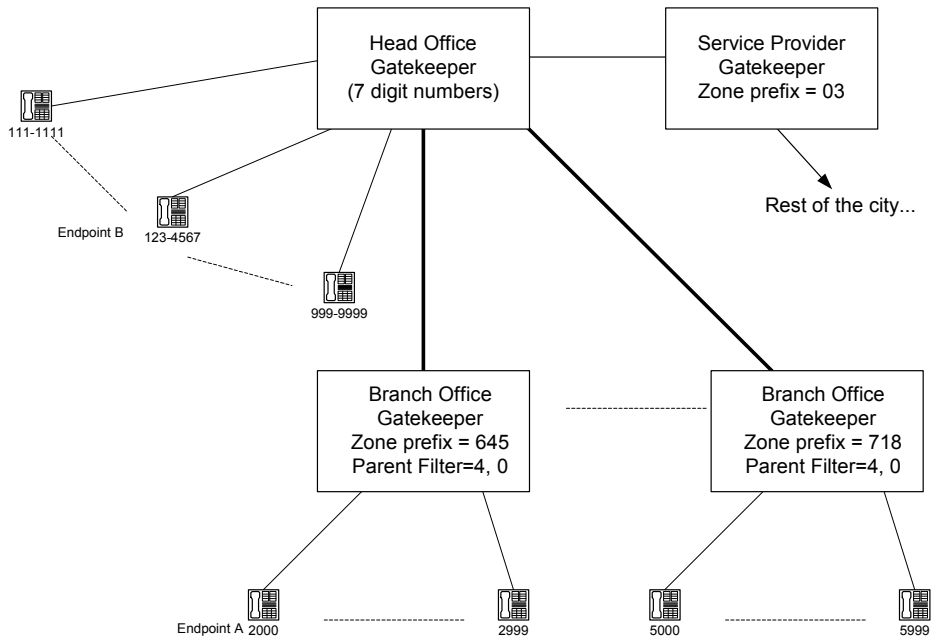

Figure D-2 *Parent Filters*

SCENARIO 2

1. Endpoint A dials 03-512-776-888.
2. The Branch Office gatekeeper searches its children and neighbors but does not find an “03” match.
3. Because one of the parent filters is 0 the Branch Office gatekeeper sends an LRQ to the Head Office gatekeeper.
4. The Head Office gatekeeper searches its neighbors and finds Service Provider with prefix 03.
5. The Head Office gatekeeper routes the call to the Service Provider with prefix 03.
6. The Service Provider connects the call to the dialed endpoint.

SCENARIO 3

1. Endpoint A dials 11-512-776-888.
2. The Branch Office gatekeeper searches its children and neighbors but does not find an “11” match.
3. Because none of the parent filters begins with 1, the Branch Office gatekeeper cannot match the call and the call fails.

IMPLEMENTATION EXAMPLE

The diagram on the following page is an example of a LifeSize Gatekeeper Dial Plan implementation in a hierarchical network.

Note The dotted lines indicate Neighbor Gatekeepers.

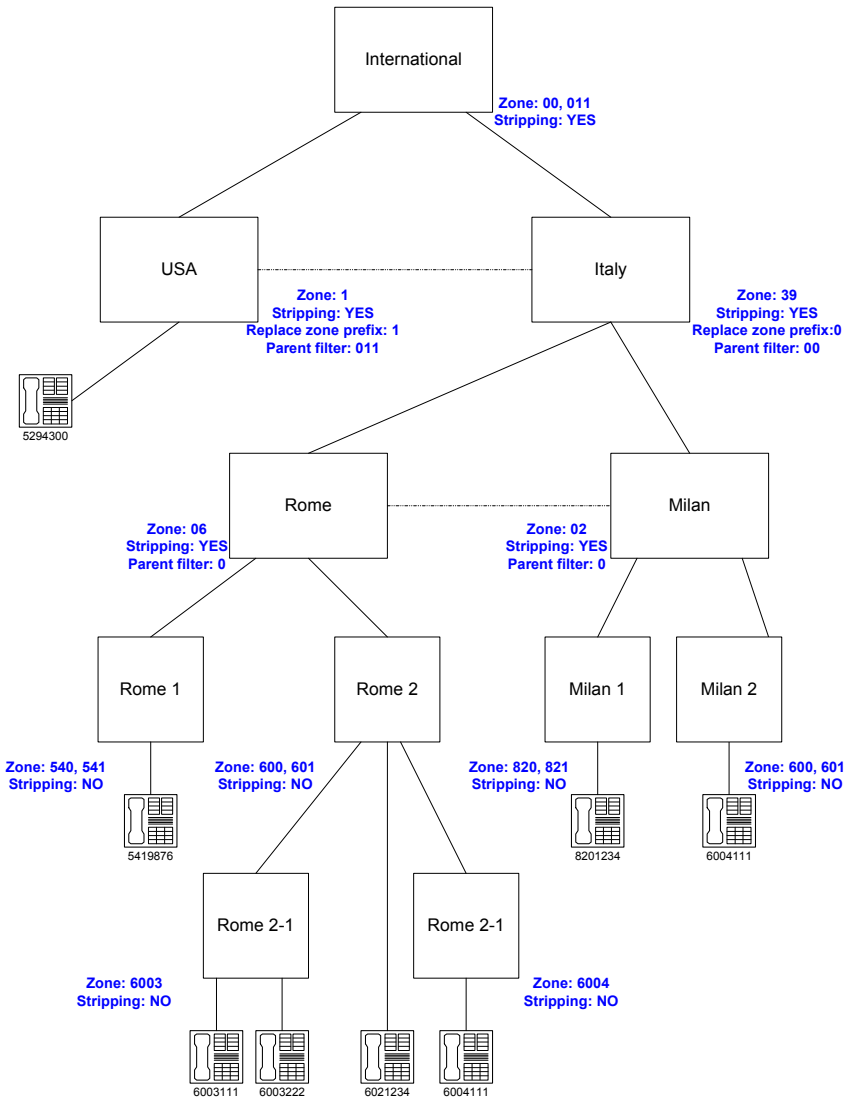

Figure D-3 *Implementation Example*

APPENDIX E

PREDEFINED ENDPOINT AUTHENTICATION BY ALIAS

WHAT'S IN THIS APPENDIX

This appendix describes how to specify the number alias matches necessary for successful authentication and registration of predefined endpoints. This appendix includes the following:

- Before You Begin
- Alias Authentication in DHCP Mode
- Alias Authentication in non-DHCP Mode
- Alias Authentication in DHCP Mode using LDAP
- Alias Authentication in non-DHCP Mode using LDAP
- Examples

BEFORE YOU BEGIN

Before you begin, note the following:

- Both the **Basics** and **LDAP** sections of the **Settings** tab include the **Number of aliases to authenticate in DHCP environment** and the **Number of aliases to authenticate in non-DHCP environment** options.
- In the **Basics** section
  - The **Number of aliases to authenticate in DHCP environment** option is enabled only when the **DHCP environment in the zone** option is checked, and when **Only predefined endpoints** is selected in the **Who can register** field.

  - The **Number of aliases to authenticate in non-DHCP environment** option is enabled only when the **DHCP environment in the zone** option is unchecked, and when **Only predefined endpoints** is selected in the **Who can register** field.
- In the **LDAP** section
  - The **Number of aliases to authenticate in DHCP environment** option is enabled only when the **Authenticate registrations with LDAP server** option is checked, and when the **DHCP environment in the zone** option is checked in the **Basics** section.
  - The **Number of aliases to authenticate in non-DHCP environment** option is enabled only when the **Authenticate registrations with LDAP server** option is checked, and when the **DHCP environment in the zone** option is unchecked in the **Basics** section.

Note For more information about DHCP, see DHCP environment in the zone on page 48.

Alias Authentication in DHCP Mode

This procedure describes how you specify the number of aliases to be matched for authentication in DHCP operation mode.

To specify the number of aliases to be matched in DHCP mode

1. In the **Basics** section of the **Settings** tab, check the **DHCP environment in the zone** option.
2. Set the **Who can register** field to **Only predefined endpoints**.

   The **Number of aliases to authenticate in DHCP environment** option is enabled.
3. Type the number of alias to be matched in the **Number of aliases to authenticate in DHCP environment** field. The number must be 1 or greater.

4 Configure predefined endpoints in the **Predefined Endpoint Properties** dialog box.

Open the **Predefined Endpoint Properties** dialog box by clicking the **Add Predefined** button in the **Endpoints** section of the **Endpoints** tab. For information about configuring predefined endpoints, see Adding or Modifying a Predefined Endpoint on page 130.

ALIAS AUTHENTICATION IN NON-DHCP MODE

This procedure describes how you specify the number of aliases to be matched for authentication in non-DHCP operation mode.

To specify the number of aliases to be matched in non-DHCP mode

1 In the **Basics** section of the **Settings** tab, uncheck the **DHCP environment in the zone** option.

2 Set the **Who can register** field to **Only predefined endpoints**.

The **Number of aliases to authenticate in non-DHCP environment** option is enabled.

3 Type the number of alias to be matched in the **Number of aliases to authenticate in non-DHCP environment** field. The number must be 0 or greater.

When 0, endpoint authentication is performed according to IP address only.

Note When the **Number of aliases to authenticate in non-DHCP environment** field is set to 0, and a predefined endpoint A exists with assigned aliases, an endpoint B with the same IP address as A can register successfully. Endpoint B can register without any matching aliases.

---

4 Configure predefined endpoints in the **Predefined Endpoint Properties** dialog box.

Open the **Predefined Endpoint Properties** dialog box by clicking the **Add Predefined** button in the **Endpoints** section of the **Endpoints** tab. For information about configuring predefined endpoints, see Adding or Modifying a Predefined Endpoint on page 130.

Alias Authentication in DHCP Mode using LDAP

This section describes how you specify the number of aliases to be matched for authentication when using the LDAP server in DHCP operation mode.

Note For more information about DHCP, see DHCP environment in the zone on page 48.

To specify the number of aliases to be matched using LDAP in DHCP mode

1. In the **Basics** section of the **Settings** tab, check the **DHCP environment in the zone** option.
2. In the **LDAP** section of the **Settings** tab, check the **Connect to LDAP server** option and type the LDAP server details in the relevant fields. For more information about configuring the LDAP server, see LDAP on page 71.
3. Check the **Authenticate registrations with LDAP server** option.

   The **Number of aliases to authenticate in DHCP environment** option is enabled.
4. Type the number of alias to be matched in the **Number of aliases to authenticate in DHCP environment** field. The number must be 1 or greater.
5. Configure predefined endpoints in the **Predefined Endpoint Properties** dialog box.

   Open the **Predefined Endpoint Properties** dialog box by clicking the **Add Predefined** button in the **Endpoints** section of the **Endpoints** tab. For information about configuring predefined endpoints, see Adding or Modifying a Predefined Endpoint on page 130.

Alias Authentication in non-DHCP Mode using LDAP

This section describes how you specify the number of aliases to be matched for authentication when using the LDAP server in non-DHCP operation mode.

Note For more information about DHCP, see DHCP environment in the zone on page 48.

To specify the number of aliases to be matched using LDAP in non-DHCP mode

1. In the **Basics** section of the **Settings** tab, uncheck the **DHCP environment in the zone** option.
2. In the **LDAP** section of the **Settings** tab, check the **Connect to LDAP server** option and type the LDAP server details in the relevant fields. For more information about configuring the LDAP server, see LDAP on page 71.
3. Check the **Authenticate registrations with LDAP server** option.

   The **Number of aliases to authenticate in non-DHCP environment** option is enabled.
4. Type the number of alias to be matched in the **Number of aliases to authenticate in non-DHCP environment** field. The number must be 0 or greater.

   When 0, endpoint authentication is performed according to IP address only.

Note When the **Number of aliases to authenticate in non-DHCP environment** field is set to 0, and a predefined endpoint A exists with assigned aliases, an endpoint B with the same IP address as A can register successfully. Endpoint B can register without any matching aliases.

5. Configure predefined endpoints in the **Predefined Endpoint Properties** dialog box.

   Open the **Predefined Endpoint Properties** dialog box by clicking the **Add Predefined** button in the **Endpoints** section of the **Endpoints** tab. For information about configuring predefined endpoints, see DHCP environment in the zone on page 48.

EXAMPLES

Table E-1 shows examples of registration attempts using the **Number of aliases to authenticate** options.

Table E-1 *DHCP Registration Examples*

Number of aliases to authenticate in DHCP/non-DHCP environment	Number of aliases assigned to predefined endpoint	Number of aliases with which endpoint attempts to register	Registration succeeds/fails
4	3	3	Succeeds
4	3	2	Fails
2	5	2	Succeeds

APPENDIX F

TROUBLESHOOTING THE LIFESIZE GATEKEEPER

This section covers problems you might encounter when configuring, operating and managing the LifeSize Gatekeeper and provides suggested actions you can perform to solve the problems.

This section describes the following topics:

- Resolving Endpoint Registration Failure on page 322
- Resolving Endpoint Unregistration/Reregistration on page 323
- Resolving H.323 Entity Registration Failure on page 323
- Resolving Endpoint Connectivity Problems on page 324
- Resolving Failure to Connect with the LDAP Server on page 324
- Resolving Call Failure to Endpoints on page 325
- Resolving Failure of Calls to the LifeSize Multipoint or LifeSize Gateway on page 326
- Resolving Call Disconnection on page 327
- Resolving Make Call Option Failure on page 327
- Resolving Forwarding Rule Failure on page 327
- Resolving Group Bandwidth Limitation Failure on page 328
- Resolving Alternate Gatekeeper Option Failure on page 328

Resolving Endpoint Registration Failure

This section describes what to do if terminals, LifeSize Multipoints or LifeSize Gateways fail to register with the LifeSize Gatekeeper.

Possible Causes	Verification Steps
The endpoint Gatekeeper IP address and RAS port are configured incorrectly.	Verify that the Gatekeeper IP address and RAS port are configured correctly in the endpoint.
The endpoint E.164 alias or IP address are configured incorrectly.	Verify that the endpoint is assigned a: ■ Unique E.164 alias ■ Unique IP address Verify that the endpoint is online.
The **Who can register field** at Gatekeeper > Settings > Basics is set to **No endpoints**.	Change the **Who can register field** to either **Everyone** or **Only predefined endpoints**.
The **Who can register** field in Gatekeeper > Settings > Basics is set to **Only predefined endpoints**.	Verify that the endpoint is predefined in the LifeSize Gatekeeper.
The **Authenticate registrations with LDAP server** option is checked at Gatekeeper > Settings > LDAP.	Add endpoint aliases to the LDAP Static Information Schema.
The endpoint tries to register to the LifeSize Gatekeeper using the wrong Gatekeeper identifier.	Verify that the Gatekeeper ID in the endpoint is correct for the LifeSize Gatekeeper.

Resolving Endpoint Unregistration/ Reregistration

This section describes what to do if endpoints spontaneously unregister from or reregister to the LifeSize Gatekeeper.

Possible Causes	Verification Steps
Duplicate IP address or E.164 alias.	Verify that the IP address and E.164 alias are unique.
TTL expires/network latency.	Increase the value in the **Multiply TTL by** field at Gatekeeper > Settings > Advanced. If this does not help, perform the following: ■ Uncheck the **Enable TTL** option at Gatekeeper > Settings > Advanced. ■ Uncheck the **Check that endpoint is online every *n* seconds** option at Gatekeeper > Settings > Advanced.

Resolving H.323 Entity Registration Failure

This section describes what to do if an H.323 entity fails to register with the LifeSize Gatekeeper.

Note This issue occurs when the H.323 entity has more than one IP address (for example, the LifeSize Multipoint IVR cannot register to the LifeSize Gatekeeper along with its LifeSize Multipoint).

Possible Causes	Verification Steps
The LifeSize Gatekeeper does not support a DHCP environment.	Verify that the **DHCP environment in the zone** option is checked at Gatekeeper > Settings > Basics.

Resolving Endpoint Connectivity Problems

This section describes what to do if you experience endpoint connectivity problems.

Possible Causes	Verification Steps
IP connectivity between the LifeSize Gatekeeper and the endpoint.	Verify that you can access the LifeSize Gatekeeper using an ICMP echo request (ping).
The endpoint registers with a different network interface than the network interface configured in the LifeSize Gatekeeper.	■ Verify that the LifeSize Gatekeeper identifies the network interfaces (IPs) that exist in the network, using the **Bind to specific IP** drop-down list at Gatekeeper > Settings > Basics. ■ Reset the LifeSize Gatekeeper host machine if an IP address was added to the machine.
LAN/cable problem	■ Verify the switch port settings. ■ Try another Ethernet cable.

Resolving Failure to Connect with the LDAP Server

This section describes what to do if the LifeSize Gatekeeper fails to connect to the LDAP server.

Possible Causes	Verification Steps
The LDAP server is offline.	Verify that the LDAP server is up and running.
The LDAP server has incorrect TCP/IP settings.	Verify that the correct LDAP server IP address is configured at Gatekeeper > Settings > LDAP.
The Gatekeeper schema is not built on the LDAP server.	Build the Gatekeeper schema on the LDAP server tree.
LifeSize Gatekeeper authentication against the LDAP server schema fails.	Use the appropriate root node, user name and password as defined in the LDAP Directory server.

Possible Causes	Verification Steps
The LifeSize Gatekeeper connection to the LDAP server is marked as “Failed”.	Reset the connection to LDAP as follows: ■ Uncheck the **Connect to LDAP server** option at Gatekeeper > Settings > LDAP. ■ Click **Upload**, then re-check **Connect to LDAP server**. ■ Click **Upload** again.

Resolving Call Failure to Endpoints

This section describes what to do if calls to endpoints via the LifeSize Gatekeeper fail.

Possible Causes	Verification Steps
The called endpoint is not registered to the local LifeSize Gatekeeper or to any other LifeSize Gatekeeper.	■ Verify that the endpoint is listed in the Endpoints table of the local LifeSize Gatekeeper and other LifeSize Gatekeeper installations in the network (if they exist). ■ If the endpoint is not registered, perform the steps described at Resolving Endpoint Registration Failure on page 322.
The dialed number contains a service prefix as a subset.	Verify that the number you dialed does not contain any service prefix which is listed in the LifeSize Gatekeeper Services table.
The endpoint you are calling is busy or not configured to Auto Answer incoming calls.	■ Wait for the endpoint to become available. ■ Wait until the call is answered.
There is a conflict between the endpoint E.164 alias and the LifeSize Multipoint/ LifeSize Gateway service prefix.	Ensure that the endpoint E.164 alias and the LifeSize Multipoint/LifeSize Gateway prefix are not the same or a subset of each other.
No calls successfully connect.	Verify that the **Accept calls** option is checked at Gatekeeper > Settings > Calls.

Possible Causes	Verification Steps
If bandwidth rules are used, all the bandwidth rules that apply to this call must be satisfied for the call to succeed. There may be one rule that exceeds its bandwidth.	■ Check which rules apply to this call. ■ Check the capacity of each rule. ■ Verify that both endpoints are registered with the LifeSize Gatekeeper.
If bandwidth rules are used, there may not be enough bandwidth for incoming calls in the zone to which you are calling due to the bandwidth reserved for outgoing calls.	■ Check the inter-zone bandwidth rules for the zone to which you are calling. ■ Check the rules capacity. ■ Check how much bandwidth is reserved for outgoing calls.

Resolving Failure of Calls to the LifeSize Multipoint or LifeSize Gateway

This section describes what to do if calls to the LifeSize Multipoint or LifeSize Gateway via the LifeSize Gatekeeper fail.

Possible Causes	Verification Steps
The LifeSize Multipoint or LifeSize Gateway service you are calling is unavailable.	Verify whether: ■ The service you wish to use is listed in the LifeSize Gatekeeper Services table. ■ The service you dialed is supported by the corresponding LifeSize Multipoint or LifeSize Gateway (at Gatekeeper > Endpoints > Type or Gateway Properties > Services > Supported Services). ■ There are no services duplicated between the LifeSize Multipoint and LifeSize Gateway. ■ There are enough resources available for the service you wish to use.

Possible Causes	Verification Steps
The calling endpoint is not allowed to use the called LifeSize Multipoint or LifeSize Gateway service.	Verify that the endpoint is allowed to call the requested LifeSize Multipoint or LifeSize Gateway service (at Gatekeeper > Endpoints > Endpoint Properties > Services > Allowed Services).

Resolving Call Disconnection

This section describes what to do if calls disconnect without any obvious cause.

Possible Causes	Verification Steps
The LifeSize Gatekeeper is configured to check that calls are active every few seconds.	Disable the **Check that call is active every *n* seconds** option at Gatekeeper > Settings > Calls.
LifeSize Gatekeeper checks terminal registrations through TTL and unregistered endpoints which fail to re-register when their TTL expires.	■ Increase the value in the Multiply TTL by field at Gatekeeper > Settings > Advanced. ■ If this does not help, uncheck the **Enable TTL** option at Gatekeeper > Settings > Advanced.

Resolving Make Call Option Failure

This section describes what to do if the Make Call option fails to operate correctly.

Possible Causes	Verification Steps
LifeSize Gatekeeper Routing mode is configured to either **Direct** or **Call Setup (Q.931)** mode.	Change the **Routing mode** option to **Call Setup (Q.931) and Call Control (H.245)** at Gatekeeper > Settings > Calls.

Resolving Forwarding Rule Failure

This section describes what to do if LifeSize Gatekeeper Forwarding rules fail to operate correctly.

Possible Causes	Verification Steps
LifeSize Gatekeeper Supplementary Services are disabled.	Verify that the Forwarding rules options are checked at Gatekeeper > Settings > Supplementary Services.
The H.323 entity does not send the correct clear cause number to the LifeSize Gatekeeper.	Verify that the H.323 entity sends the correct clear cause number in the ethereal log.

Resolving Group Bandwidth Limitation Failure

This section describes what to do if bandwidth limitation for a group does not operate correctly.

Note This issue occurs when you have defined a bandwidth limitation for a group. However, an endpoint that belongs to this group can make a call at a higher bandwidth.

Possible Causes	Verification Steps
An endpoint receives permissions from all the groups it belongs to.	■ The highest permission applies. ■ Remove that endpoint from the high bandwidth group.

Resolving Alternate Gatekeeper Option Failure

This section describes what to do if the Alternate Gatekeeper feature fails to operate correctly.

Possible Causes	Verification Steps
Alternate Gatekeeper is not available.	Verify that the **Use Alternate Gatekeeper** option is enabled at Gatekeeper > Settings > Alternate Gatekeeper.

Possible Causes	Verification Steps
When the Master is down, the Slave does not become a Master.	For both Gatekeepers check the following: ■ Verify that you can access the Probe IP from each LifeSize Gatekeeper using an ICMP echo request (ping). ■ Verify that the Alternate Gatekeeper Native IP field holds the IP address of the second (Alternate) LifeSize Gatekeeper. ■ Verify that the license details and Gatekeeper ID for each LifeSize Gatekeeper are identical.
LifeSize Gatekeeper abnormally changes its mode from Master to Slave.	Increase the ICMP echo request (ping) timeout in the LifeSize Gatekeeper registry.
Both LifeSize Gatekeeper instances remain in Slave mode and neither becomes a Master.	■ Verify that the Public IP address is not already occupied by another entity on the network. ■ Verify that the LifeSize Gatekeeper is set to the correct NIC card. Check at Gatekeeper > Settings > Basics that the **Bind to specific IP** option is set correctly. ■ This problem may occur when the LifeSize Gatekeeper is installed on a machine with several NIC cards.
After the LifeSize Gatekeeper Slave becomes a Master, it does not behave as the old Master	Verify that both LifeSize Gatekeeper configurations are the same.

INDEX

A

Alert indications 67
Aliases
  additional alias 196
  authentication
    in DHCP mode 49
    in DHCP mode with LDAP 76
    in non-DHCP mode 49
    in non-DHCP mode with LDAP 77
  destination endpoint alias 196, 198
  endpoint alias 134, 135
  format restrictions 118, 120
  forwarded-to endpoint alias 212, 217
  forwarding endpoint alias 211, 215
  resolving queries 50, 106, 113, 224
  selecting alias type 135, 211, 213, 216, 217
  source endpoint alias 195, 197
Alternate Gatekeeper 10, 95, 99
  enabling 102, 103
  inter-gatekeeper communication port 103
  IP Release 101
  Native IP 102
  ping interval 103
  Probe IP 103
  Public Gatekeeper IP 103
  Windows IP addressing 96
ARQ 22
  Pre-grant ARQ 104
Authorization of endpoints by external server 15, 81
Auto Refresh 127, 192
Automatic e-mail address generation 11, 83, 85, 86
Automatic MCU service registration 11

B

Bandwidth
  approved 195, 196
  requested 195
  total 195
Bandwidth management
  inter-subzone 184
  inter-zone 44
  within group 146
Bandwidth Policy tab 169
Billing 65–66, 67
Built-in policies 3
Built-in services 156

C

Call Control tab 191
Call Fallback 16, 208, 213
Call Setup
  H.245 address in Setup message 52
  immediate Call Proceeding 52
Call signaling
  address 195, 196
  channels 22
Caller ID presentation 80
Calls 50
  accept 52
  block when dialed with IP address only 15, 53
  call signaling address 195, 196
  caller ID 195
  checking a call is active 52
  conference ID 194

current number ongoing *vs* maximum permitted 44
disconnecting a call 193
disconnecting all calls 193
establishment 21
Forward On Busy (H.450.3) 60, 207, 212
Forward On No Answer (H.450.3) 61, 207, 212
forwarded-to alias type 213, 217
forwarding a 1B call to another terminal via a gateway 157
forwarding all calls to another IP terminal 157
maximum number 55
remote alias 196
termination 26
Transfer (H.450.2) 60
Unconditional Forward (H.450.3) 61, 207, 212
Capacity 54
CDR 5, 65–67
alias tags 286
basics 277
billing port number 67
billing server IP address 67
call model tags 287
endpoint type tags 287
field format 278
field numeric options 286
field tags and default attributes 280
field types 278
file name extension 66
file name prefix 66
file size 66
fixed length fields 278
Generator tags 290
H.450 Call record type tags 291
H.450 Forward type tags 290
Party Number tags 286
Reason tags
ARJ 288
Release 288
Record type tags 290
samples 292
send to server 66
simple routed call 292
total space 66
transferred call 293
variable length fields 279
Central Database 87–88
information retrieval 88, 116, 168, 227
Child Gatekeepers 228, 230
Child prefixes 231
Cisco Proxy 6, 110
enabling 116, 227
unknown zones 105
Conference Hunting 7, 163
Configuration interface 34, 41
Global tabs 38
Control channels 26

D

Databases
Central Database 87–88
information retrieval 88, 116, 168, 227
LDAP
information retrieval 79, 116, 227
Debug level 64
Destination zone 288
DHCP
DHCP environment in the zone 48
Dial Plan 10, 57
aliases that are not numbers 306
exit zone prefixes 308
gatekeeper topology 303
global services 307
local services 307
number of digits 306
numbering 305, 306
parent filters 311
prefixes 306
selecting a version 47
services 307
Services tab in version 2 164
stripping 308
topology 303, 304, 305
Zone Prefixes 308
Disconnecting a call 193

Disconnecting all calls 193
DNS 10, 83–86
DRQ 26

E

E-mail address generation 11, 83, 85, 86
Endpoints
  allowed services 139
  authorization via external server 15, 81
  checking an endpoint is online 105
  current number registered *vs* maximum permitted 44
  Force Direct Mode 108
  Force Routed Mode 78
  forwarding extension 212, 217
  in-zone non-predefined endpoints 164
  locating endpoints 78, 128, 201
  make predefined 140
  modify registration IP address 132
  modifying the properties of an online endpoint 138
  out-of-zone endpoints 164
  predefined 129, 130, 132
    edit predefined data 130, 140
  registration
    maximum number 55
    policy 48
  remote alias 196
  specifying type 131
  supported services 139
  Time To Live (TTL) 106
    TTL Resiliency 12
  unregistering 130
    endpoint-initiated unregistration 26
  unregistering all 130
  user name 236, 237
Endpoints tab 125
Enhanced services 3
Event Log tab 233
Exit zone prefixes *See also* Dial Plan 159, 308
External API 15, 81

F

Fallback 16, 208, 213
Filters 220, 222, 311
  adding 223
  modifying 223
Fixed Calling Party Number 13, 53, 107, 136
Forward & Fallback tab 207
Forwarding 156, 207, 208
  endpoint extension 212, 217
  Forward On Busy (H.450.3) 60, 207, 212
  Forward On No Answer (H.450.3) 61, 207, 212
  forwarded-to alias type 213, 217
  forwarding a 1B call to another terminal via a gateway 157
  forwarding all calls to another IP terminal 157
  non-H.450.3 forwarding 132
  Unconditional Forward (H.450.3) 61, 207, 212

G

Gatekeeper identifier 222
  configuring 47
Gatekeeper identifier indication 37
Gateways
  forwarding a 1B call to another terminal via a gateway 157
  forwarding extension 212, 217
  remote alias 196
  stripping prefixes 58, 59
Global service prefixes 163, 165, 167, 307
Group Hunting 7, 299, 300
Groups 140–153

H

H.235 Security 93
H.235 security 10
  enabling 94
H.245
  H.245 address in Setup message 52
  routing H.245 Control channels 26

tunneling 13
H.245 Proxy 51
logging 64, 65
H.255
routing H.225.0 Call Signaling channels 22
H.323 Gatekeeper procedures 21
Admission Request (ARQ) 22
Disengage Request (DRQ) 26
Gatekeeper Discovery 21
Gatekeeper Registration 22
Location Request (LRQ) 22
Unregistration Request (URQ) 26
H.323 Gatekeepers 20
destination zone 288
unregistration 26
H.323 Recommendation 19
H.341 MIB support 5
H.350 Internet2 LDAP schema 15, 79
H.450.2 Transfer 60
H.450.3
Forward On Busy 60, 207, 212
Forward On No Answer 61, 207, 212
non-H.450.3 forwarding 132
Unconditional Forward 61, 207, 212
H.450.3 Call Forwarding rules 211
Hierarchical gatekeeper structure 219
Hierarchy
adding a Child Gatekeeper 230
adding a child prefix 231
adding a gatekeeper IP address 230
adding a Neighbor Gatekeeper IP address 226
adding a Parent Gatekeeper IP address 221
Central Database
information retrieval 227
Child Gatekeepers 228
child prefixes 231
Cisco Proxy 227
Gatekeeper port number 221
LDAP 227
locating endpoints 128, 201
modifying a Child Gatekeeper 230
modifying a child prefix 231
modifying a gatekeeper IP address 230
modifying a Neighbor Gatekeeper IP address 226
modifying a Parent Gatekeeper IP address 221
Neighbor Gatekeeper port number 221
Neighbor Gatekeepers 223
parent filters 222, 223
Parent Gatekeepers 220, 221
resolving alias queries with Neighbor Gatekeepers 224
Hierarchy tab 220

I

Installation
Internet Information Server (IIS) 4 subcomponents 270
SNMP 268
Internet Information Server (IIS) 4 subcomponents 270
IP addresses
billing server IP address 67
block calls when dialed with IP address only 15, 53
endpoint registration IP 132
Native IP 102
Probe IP 103
Public Gatekeeper IP 103
range restrictions 121, 122
IP Release 101

L

LDAP 10, 71
alias authentication
in DHCP mode 76
in non-DHCP mode 77
basics 244
binding the server 264
Configuration Tool 248
configuring the server 247
connecting to server 74, 76, 83
deactivating access to the server 79, 81
information retrieval 79, 116, 227

Internet2 schema (H.350) 15, 79
LDAP Tree 245
Gatekeeper List Tree 246
locating 253
modifying 254
Online Information Tree 246
Static Information Tree 246
resolving alias queries 78
server address 74
server user name 74, 83
updating server with online information 78
LDAP Configuration Tool 248
LDAP servers
iPlanet Directory Server 5.1 253
Netscape Directory Server 4.1 253
OpenLDAP 244, 260
Licensing
viewing licensing details 240
Line Hunting 7
Logging 10, 62–64, 65
event log 233
LRQ 22
hop count 59
LRQ Policy
LDAP 78
multicast 50
Neighbor Gatekeepers 113, 224
simultaneous 106

M

Make Call 14, 34, 193, 197, 199
MIB 5, 240
multicast 50

N

Native IP 102
Neighbor Gatekeepers 111, 114, 223, 226
port number 221, 230
resolving alias queries 113, 224
Neighbors tab 112

O

Online endpoints
modifying properties 138

P

Parent filters 220, 222, 311
adding 223
modifying 223
Parent Gatekeepers 220, 221
Passwords
adding or modifying user details 237
SQL server user 88
user 237
Policies
built-in 3
Ports
billing server 67
connection to LDAP server 74, 83
Gatekeeper 221
inter-gatekeeper communication port 103
Neighbor Gatekeeper 221, 230
Predefined endpoints 125
add predefined 129, 130
edit predefined 130
make predefined 140
modifying predefined properties of an online endpoint 140
remove predefinition 130
Prefixes *See also* Dial Plan 163, 306
child prefixes 231
global service prefixes 167, 307
service prefixes 163
stripping 58, 59, 308
Zone Prefixes 115, 157, 226, 308
Probe IP 103
Proxy
Cisco Proxy 6, 110
enabling 116, 227
unknown zones 105
H.245 Proxy 51
logging 64, 65
Public Gatekeeper IP 103

R

RADIUS server 15, 89
RAI/RAC 7
RAS capabilities 27
Registration
  maximum number 55
  policy 48
  restrictions 14, 117
    alias format 118, 120
    IP range 121, 122
Registration Restrictions tab 117
Resolution of aliases 9
  LDAP 78
  multicast 50
  Neighbor Gatekeepers 113, 224
  simultaneous 106
Routing
  Direct Mode 22
  routing H.245 Control channels 26
  routing H.255.0 22
  Routing Mode 22, 51, 101
    call model 195
    Force Direct Mode 108
    Force Routed Mode 78

S

Security 10, 93
  adding or modifying user details 237
  enabling H.325 security 94
Security Passwords tab 235
Services 155, 165, 307
  allowed 139
  built-in 156
  enhanced 3
  global services 163, 167
  prefixes 163
  supported 139
  user-defined 156, 162
Services tab 159
  in Dial Plan version 2 164
Settings tab 45
Sidebar 35
SNMP
  installing on Windows 2000 268
  traps 67
SQL
  server 88
Status tab 43
Stripping 59, 308
Subzones 170–174
Supplementary Services 5, 59
  Forward On Busy (H.450.3) 60, 207, 212
  Forward On No Answer (H.450.3) 61, 207, 212
  non-H.450.3 forwarding 132
  Transfer (H.450.2) 60
  Unconditional Forward (H.450.3) 61, 207, 212

T

Third Party Call Control 14, 193, 197, 199, 200
  status of calls 199
  via external server 15, 81
  viewing calls in progress 194, 204
Time To Live (TTL) 106
  TTL Resiliency 12
Toolbar 37
Transfer (H.450.2) 60

U

Unregistration
  endpoint-initiated unregistration 26
  gatekeeper-initiated unregistration 26
URQ 26
User-defined services 156, 162

V

Version
  Gatekeeper version 240
  License key 240
  MIB version 240
Version tab 239

W

Web interface 5, 31, 32
Wildcard digit manipulation 10

X

XML call control 15, 81

Z

Zone Prefixes *See also* Dial Plan 115, 226, 308
  exit zone prefixes 308
  stripping 58, 59
  Zone Prefix 1 and 2 Service 157
Zones
  destination zone 288